



AIRA
AMERICAN IMMUNIZATION
REGISTRY ASSOCIATION

Discovery Session

Securing What Matters: A First Look at the *2026 Security Guidance for IIS*

September 28, 2026 | 4:00 p.m. ET



Today's Presenters

- **Eric Heflin, MA**, Consultant, AIRA
- **Erin Roche, MPH, MS, CPH**, Consultant, AIRA
- **Austin Fuoco**, IIS Deputy Manager, Philadelphia Department of Public Health



Today's Road Map

- | | | |
|---|-----------------------------------|--|
| 1 | How we got here | Why the resource became a community priority |
| 2 | Why security matters | The public health and operational case |
| 3 | How the guidance was built | A rigorous, community-informed process |
| 4 | What's inside | A guided tour of the resource |
| 5 | Putting it to work | Practical ways to get started |
| 6 | Q&A | Questions, discussion, and takeaways |



Session Objectives

Describe

Why the 2026 guidance was developed and how the IIS community helped shape it

Explain

Why IIS security matters for data, operations, resilience, and trust

Identify

The major sections, priority topics, and companion resources

Apply

Practical ways to use the guidance to assess, prioritize, and improve over time.



How We Got Here



The **Resource Development Recommendations Workgroup (RDRW)** gives the IIS community a structured way to identify and prioritize resources that need to be created or updated.



Community-Driven Process

RDRW

Identified the need for a new security resource as a community priority

Advisory Panel

Contributed diverse expertise and IIS perspectives throughout development

CDC

Provided funding support, input, and review throughout the project

IIS Community

Broadened validation before the resource was finalized

Goal: Guidance that is current, credible, and usable across diverse IIS environments



Building on the 2017 Security Guidance

Threats evolved

Cybersecurity threats are increasingly persistent, disruptive, and interconnected across healthcare and public health.

Technology evolved

Cloud services, modern software practices, third-party dependencies, and AI introduce new opportunities and new considerations.

Security practices evolved

Standards, safeguards, governance practices, and approaches to managing cybersecurity risks have continued to mature.



Why IIS Security Matters



Data

Protect sensitive information

Confidentiality, integrity, and appropriate access



Operations

Keep critical services reliable

Availability for clinical, program, and reporting needs



Resilience

Prepare for disruption

Continue critical functions and recover effectively



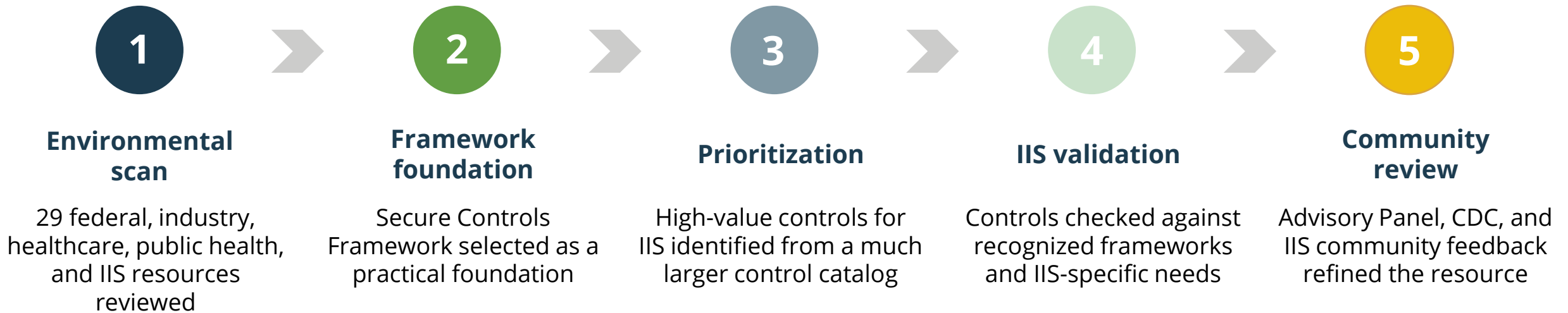
Trust

Protect confidence in IIS

Patients, providers, partners, and the public

A secure IIS helps ensure that that patients, health care providers, and public health can rely on immunization information that is available, accurate, protected, and trusted.

How the 2026 Guidance Was Developed

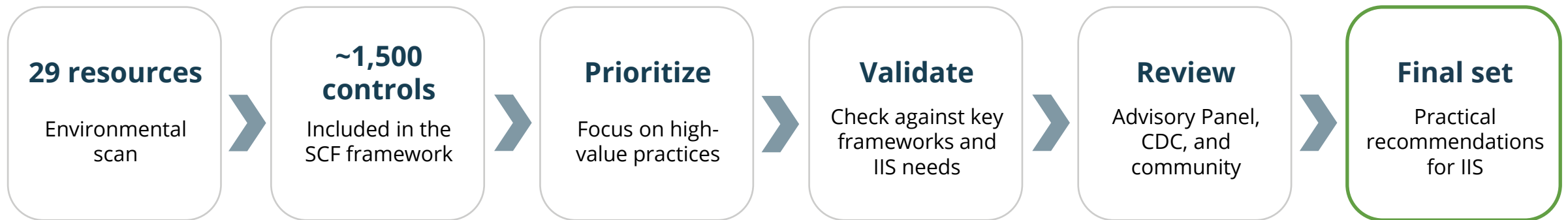


Cybersecurity controls are safeguards and practices used to reduce security risk. The goal was not to include every available control, but to identify practical recommendations with strong value for IIS programs.



From a Wide Cybersecurity Landscape to Focused IIS Priorities

The methodology was designed to make a large body of security guidance more usable.



A structured process helped narrow a broad cybersecurity landscape into practical, IIS-focused priorities.



Why the Secure Controls Framework (SCF)?

Broad coverage

Brings cybersecurity, privacy, and compliance concepts together

Cross-framework mapping

Connects to major standards, reducing manual reconciliation

Actionable detail

Offers control-level information that can support implementation

Acceptable and adaptable

Resources are openly available and can be tailored for IIS

SCF is the foundation. The guidance adds the IIS context.



What's Inside

Security fundamentals

Core concepts, terminology, legal and regulatory context

Security program

Leadership, accountability, roles, responsibilities, and risk decisions

Operational security

Day-to-day practices for systems, data, people, partners, and technology

Artificial intelligence

Cross-cutting risks and opportunities associated with AI

Business continuity + response + recovery

Preparing for disruption, responding effectively, and restoring services

Appendices

Methodology, roles, acronyms, and orientation to SCF



Designed for Real IIS Environments

Different organizational structures

Different staffing and resources

Different technology environments

Different levels of cybersecurity maturity



What that means

The guidance focuses on high-priority practices that programs can tailor to their own environment, needs, resources, and risk tolerance.

It is a guide for continuous improvement, not a one-size-fits-all checklist.

You are not expected to implement everything at once.



AIRA Guidance Built for Different Roles

EL

Executive leadership

Governance, accountability,
priorities, and resources

IIS

IIS managers / project managers

Coordination, risk-informed
planning, and road maps

IT

IIS IT implementers

Operational practices, controls,
evidence, and technical
implementation

**Security responsibilities are shared.
The guidance helps each role find the sections most relevant to its work.**



Start with the Foundation

Ch 1. Introduction

- Importance of security to IIS operations
- Purpose and desired outcomes
- Intended audience and use
- Organization and scope of the guidance

Ch 2. Security fundamentals

- Key cybersecurity concepts and terminology
- Legal and regulatory considerations
- Reference resources
- Concepts that support informed security decisions

Ch 3. Establishing & maintaining a security program

- Governance and leadership
- Roles and responsibilities
- Risk management
- Accountability and coordination
- Ongoing prioritization and improvement



How Chapter 3 is Structured

Governance and accountability

Effective security governance establishes clear direction, oversight, and accountability for IIS security.

It also helps programs define priorities, make informed decisions, and ensure appropriate resources are considered.

Roles and risk management

Clearly defined roles help ensure the right people are involved in security decisions and understand their responsibilities.

A risk-informed approach helps programs identify concerns, evaluate priorities, and determine where to focus security efforts.

How to use Chapter 3

Understand the environment

Know the requirements, systems, data, dependencies, and partners.



Assess and prioritize risk

Identify risks and focus attention where it matters most.



Plan and improve over time

Set realistic priorities, assign ownership, and revisit progress.



How Chapters 4-6 Are Organized

IIS-focused organization

Controls are grouped into IIS-relevant security topics.

The tables also connect recommended practices to the applicable SCF control and, where relevant, related IIS RTM requirements.

Practical considerations for IIS

Each topic includes practical considerations that translate the recommended security practices into an IIS context.

How to use Chapters 4-6

Find the relevant topic

Start with the security area that aligns with the program's need.



Review the recommended practices

Use the control tables to understand what should be in place.



Apply it to the IIS environment

Use the practical considerations to determine what implementation could look like locally.



Chapter 4: Operational Security

The day-to-day practices that protect IIS systems, data, and operations.

People & workforce

Physical
environment

Third parties

Systems & networks

Secure
development

Web applications

Change &
configuration

Identity & access

Data protection

Logging &
monitoring

The guidance connects these topics to prioritized controls and practical considerations. The Discovery Session stays at the topic level.



Chapter 5: Special Topic: Artificial Intelligence

AI creates both opportunities and security considerations for IIS programs.

Opportunities

AI is increasingly integrated into public health technologies and cybersecurity tools. It may support efficiency, analysis, and security capabilities.

Considerations

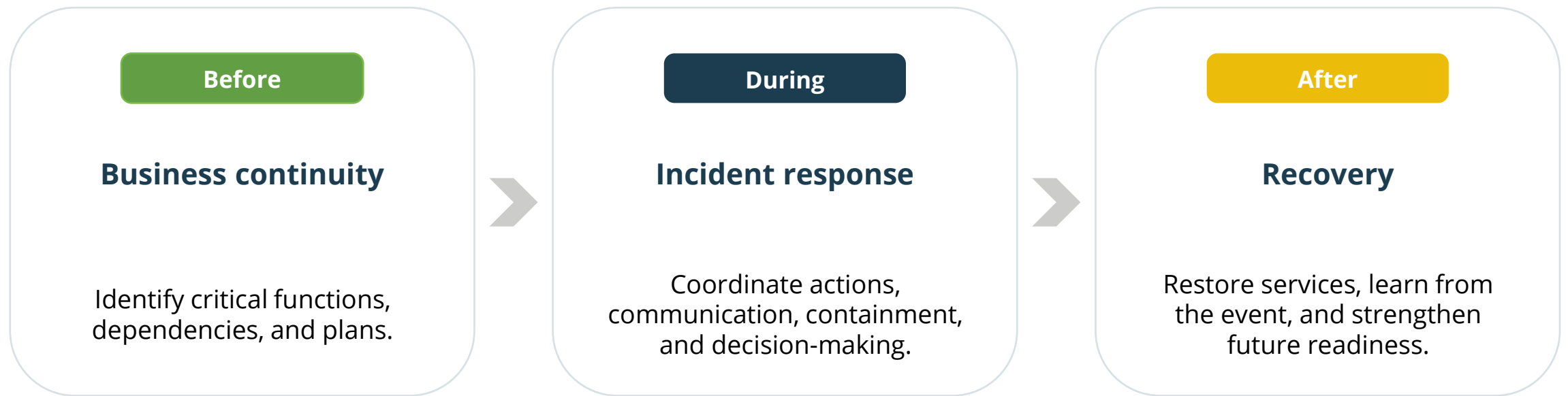
Programs should consider data protection, governance, vendor practices, accuracy, oversight, and other risks when AI touches IIS work.

The guidance treats AI as a cross-cutting security topic, not a stand-alone technology project.



Chapter 6: Business Continuity, Incident Response, and Recovery

Security also means being ready to continue and recover.



Resilience is a cycle. Preparation and learning matter as much as response.



Companion Resources

Environmental Scan

Background on the resources reviewed and why SCF was selected as the foundation.

Security Controls for IIS

A workbook that brings the IIS-specific prioritized controls together in one place.

Cybersecurity Tips

A concise, action-oriented companion for practical security reminders and discussion with a special focus on highly cost-effective approaches.

Use these resources based on your program's needs and priorities.



Quick Facts Philadelphia:

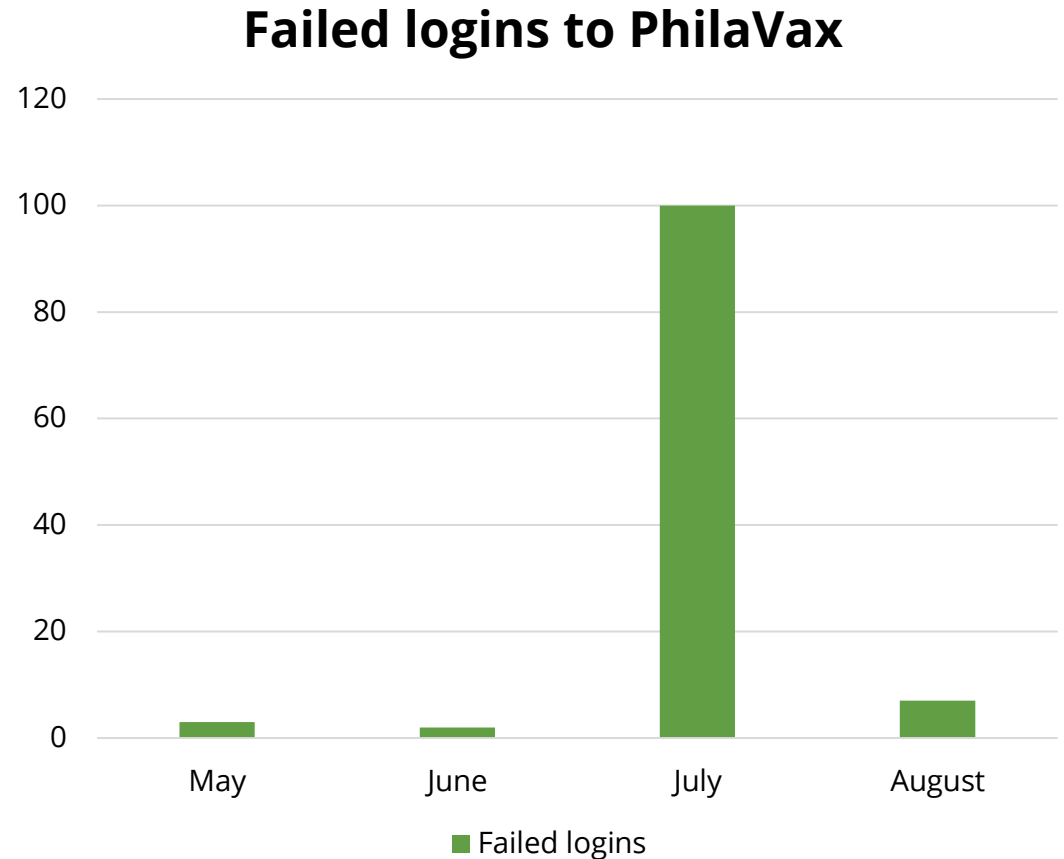
- Population: 1.5 Million
- IIS: PhilaVax
- IIS staff: 11
- Users: >2000
- Security incidents: 0



PhilaVax

Why Security Matters

- IISs have grown and evolved
- That growth makes the data in the IIS incredibly valuable to bad actors
- Makes every IIS a potential target



Why This Guidance is Exciting



Comprehensive

Covers everything from data exchange, day-to-day security, third party risk to incident response.



Flexibility

Gives you the tools to go as in-depth if you need too, but you can just pick a topic and dive right in.



Role-based

Not one size fit all. Guidance is tailored to each part of the community.



Practical

All the controls translate directly to the work you and your team already do.



Self-paced

You cannot do it all! Start with the most impactful controls and expand out to gaps or quick wins in your org.

Practical, flexible guidance that programs can use at their own pace.



Putting the Guidance to Work

Where are we now

Use the guidance to review current practices and identify strengths or gaps

What matters most

Prioritize needs based on risk, operational importance, resources, and local context

Who needs to be involved

Use the resource to support conversations with leadership, IT, privacy, vendors, and partners

What comes next

Turn priorities into a realistic security road map and revisit it regularly when conditions change

Think “next best step,” not “do everything.”



Use the Guidance as an Improvement Tool

The resource supports progress over time, not a one-time compliance exercise.

1

Understand

Know your requirements, systems, data, dependencies, and partners.

2

Assess

Review current practices, capabilities, risks, and gaps.

3

Prioritize

Focus on what matters most based on risk and local context.

4

Plan

Build a realistic security road map with ownership and next steps.

5

Improve

Monitor, revisit, and strengthen practices as conditions change.

**There is no required starting point.
Begin where the need is clearest, then keep the cycle moving.**



Three Ways to Start This Week

1

Bring the right people together

Use the guidance to strengthen governance and support conversations with program, IT, security, privacy, and vendor partners

2

Pick one priority area

Choose a section tied to a current concern, project, audit, modernization effort, or known gap

3

Document one next step

Identify an action, owner, and follow-up point. Build from there

**Security improvement is ongoing.
The goal is to make informed, risk-based progress over time.**



Key Takeaways

Community-driven

The opportunity began with a community-identified priority and was shaped through broad review

Public health essential

Security protects data, reliable operations, resilience, and trust

Practical by design

The guidance translates a complex cybersecurity landscape into IIS-relevant priorities

Built for progress

Use it to assess, prioritize, communicate, and improve over time



Technical Advisory Bulletins (TABs)

- Support HL7 2.5.1 immunization messaging
- Build on and clarify specifications in the *HL7 v2.5.1 Implementation Guide for Immunization Messaging, Release 1.5 and Addendum, October 2018*
- Each TAB addresses a specific topic

Use TABs to support the development and maintenance of HL7 exchange capabilities and interfaces, working with exchange partners as needed to test/confirm changes



Newly Updated and Published Technical Advisory Bulletins

CDS in RSP Alignment - *update*

- Updated the October 2025 document to correct a coding system identifier in the example:
 - Updated the coding system identifier in the OBX-5 fields associated with LOINC 59783-1 (Status in series) to 'LN' rather than 'LA', as 'LN' is the HL7 coding system identifier for LOINC

Submission of Self-Administered FluMist Vaccine to IIS - *update*

- Updated the July 2025 guidance to include a summary of changes for Fall 2026/Spring 2027 respiratory season
 - RXA-5: Plan for continued reporting of CVX (333) and updated NDC
 - Prepare for expanded vaccine access and reporting across the contiguous U.S. + DC

Review TABs for potential impacts to IIS interfaces, implementation practices, and testing activities.



TABs are Available in the Repository

- Available at <https://repository.immregistries.org/resource/tab-resources>

Information reported in this presentation was supported by National Center for Immunization and Respiratory Diseases (NCIRD) of the Centers for Disease Control and Prevention under award number 6 NU38OT000291-05-01. The content is solely the responsibility of the authors and does not necessarily represent the official views of CDC.

Technical Advisory Bulletins (TAB) Resources

Issued on July 15, 2025 by AIRA



OPEN RESOURCE:

- [↓ TAB Overview](#)
- [↓ TAB Query Response Flexibility](#)
- [↓ TAB Additional "Unknown" Race and Ethnicity Codes](#)
- [↓ TAB Scenarios for Updates and Queries](#)
- [↓ TAB System Entry Date/Time \(RXA-22\)](#)
- [↓ TAB Messaging Phone and Email](#)
- [↓ TAB Returning IIS Patient Immunization Record Information](#)
- [↓ TAB Messaging Non-patient Person Names in HL7](#)
- [↓ TAB Submission of Self-Administered FluMist Vaccine to IIS](#)
- [↓ TAB CDS in RSP Alignment](#)
- [↓ TAB Patient Name \(PID-5\) Updates to Support Patient Matching](#)
- [↓ TAB Acknowledgement \(ACK\) Messaging Updated Specifications and Guidance](#)



Thank you to our presenters,
and thanks to all of you for
joining us!

Please complete a brief evaluation survey

The next Discovery Session
will be on **October 26, 2026**