NewSTEPs

A Program of the Association of Public Health Laboratories™

GUIDE TO NEWBORN SCREENING RESULTS PORTALS

The development of this document was supported by the Health Resources and Services Administration (HRSA) under Cooperative Agreement #U22MC24078 for $1,500,000. This information or content and conclusions are those of the authors and should not be construed as the official position or policy of, nor should any endorsements be inferred by HRSA, HHS or the US Government.

Acknowledgements

APHL would like to recognize the following individuals that generously contributed their time and expertise to the development of this document:

- Tarence Beard, Security+, Etegrity Health Solutions
- Christianne Biggs, MS, Oregon State Public Health Laboratory (Retired)
- Amy Gaviglio, MS, CGC, Public Health Genetics Consultant, APHL

Contents

Acknowledgements 2

Executive Summary 5

Introduction 9

Methods 9

Newborn Screening Results Portals 10

- Requirements and Functionality 10
- Data Sharing Agreements 13
- Privacy and Security 17
  - Cybersecurity Threats 17
  - HIPAA Privacy Rule 17
  - HIPAA Security Rule 17
  - HIPAA Security Incident 19
  - HIPAA Security Incident Response Plan 19
  - HIPAA Breach Notification Rule 22
  - HIPAA Breach Risk Assessment 22
  - HIPAA Breach Exceptions 22
  - Breach Notification Requirements 23
  - Identity and Access Management 23
  - User Authentication 25
  - Authorization and Role Based Access Control 26
  - Facility Administrator Role 26
  - Account Provisioning/De-provisioning 27
  - Identity Proofing Assurance Level 27
  - Password Management 29
    - Single Sign-On 29
    - Self Service Password Management 29
- Report Access and Searching 30
  - Patient Searches 31
    - Matching 31
    - Patient Search Criteria 31
    - Search Errors and How to Prevent Them 32

Required Minimum Search Parameters 32
Audit Trails and Reports 34
Transitioning to use of a Remote Portal 36
Communication and Onboarding 36
Staffing 38
Future Directions 39
List of Acronyms 40
Glossary of Terms 42
List of Appendices 45
Appendix A: Examples of Data Use and Sharing Agreements 45
Appendix B: Examples of Training/Onboarding Materials 45
Appendix C: Case Studies 46
Case Studies for Report Access 46
Case Studies for Report Search Criteria 50
References 52

Executive Summary

The Association of Public Health Laboratories (APHL's) Newborn Screening Technical assistance and Evaluation Program (NewSTEPs) has developed this resource document to assist Newborn Screening Programs with implementing and maintaining result report portals. This document outlines recommendations and potential solutions, covering activities around information technology (IT) to access administration to privacy and authentication practices. Below is a summary of recommendations from each section of the document.

Document Section	Category	Recommendation
Newborn Screening Results Portals (NBSRP)	**Requirements and Functionality**	*Clearly and concretely describe the business, user and system requirements for the Newborn Screening Results Portal (NBSRP).*
		Develop a comprehensive list of requirements and desired functionality using input from a variety of stakeholders, including Newborn Screening (NBS) program staff, Information Technology (IT) staff and End-Users.
	Data Sharing Agreements	*Check with your agency to see if a data sharing agreement and policy already exists that can (or must be) used.* *If you need to create or make modifications to a data sharing agreement, make sure to include IT security and your Privacy Officer (or whoever fills that role in your NBS program) in order to make sure you have a document that maintains the security of your data, limits your liability and meets the NBS program's needs while also adhering to any federal and local requirements.*
		If you are using a vendor supplied portal [such as E-Reports (PerkinElmer) or Secure Remote Viewer (Neometrics)], check with them to see what security measures they have in place to protect the data that is being accessed.
		When creating or reviewing the agreement you will use, consider the following items: • *Method of sharing* • *Period of agreement* • *Intended Use* • *Constraints on use* • *Data confidentiality* • *Data security* • *Any legal or other requirements specific to your jurisdiction* *Some questions to consider are:* 1. *What process for authorization is required for people or organizations to access data?* 2. *Who facilitates the process?* 3. *Who maintains the process (adds and deletes users, maintains the database and audits it for access and users who should be removed)?* 4. *Does the agreement for access and use need to be legally binding?* 5. *Who needs to complete the agreement?* 6. *Does the person requesting access need authorization and/or verification from their organization?*

Document Section	Category	Recommendation
		7. Do they need to meet any specific criteria in order to access data (e.g., have a current medical license)? If so, what are the criteria? *8. In addition to the data sharing agreement to grant access, does the portal need to contain a user agreement that must be agreed to each time the user accesses the site?* *9. Are there consequences for misuse of the data and are these consequences clearly stated?* *10. How long is authorization good for?* *11. Is there a process to remove expired users or those who should no longer have access?* *12. What are the requirements for data security?* *(Questions adapted from Best Practice Guide to Applying Data Sharing Principles version: 15 March 2019 Australian Government - Department of the Prime Minister and Cabinet)*
	Privacy and Security	*Consider establishing a Cyber Security Incident Response Team (CSIRT) consisting of stakeholders within the NBS program, Laboratory Information Management Systems, Information Security Officer, Privacy Officer, General Counsel and Information Technology Department.*
		Follow NIST SP 800-61 Revision 2 "Computer Security Incident Handling Guide" and Health Insurance Portability and Accountability (HIPAA) Security Rule policies and procedures when establishing a robust Security Incident Response Plan and establish an initial security incident triage checklist.
		Conduct both periodic reviews of the security incident response plan and practice drills as effective communication across teams and coordinated timely responses help mitigate security incidents.
		Ensure employees are trained and/or periodically refreshed on HIPAA polices and guidance.
		Ensure HIPAA breach response aligns with a documented security incident response plan. This well help establish a clear and well-planned governance to a breach.
		Confirm whether your NBS program is a HIPAA-covered entity. Although some NBS programs may not be considered covered entities, NBS program leadership should strongly consider following these rules given their adoption within the healthcare industry private sector as best practices.
		Define clear procedures for who is responsible for the software maintenance, customer support, technical support, account provisioning/de-provisioning.
		Increase security awareness by training NBS program employees on what the rules are and how to abide by them.
		Establish a process to review and maintain the policies and procedures to stay up to date and current with the HIPAA Privacy and Security Rules.

Document Section	Category	Recommendation
	User Authentication	*Implement Multi-Factor Authentication (MFA) such as two-factor authentication: "Something you know" and "Something you have."*
		When using "Something you have" authentication factor, consider incorporating a mobile authentication application, e.g., Microsoft Authenticator and avoid using Short Messaging Service (SMS).
		Follow NIST SP 800-63-3 guidelines for username/password.
	Facility Administrator	*Consider establishing and implementing a robust Role Based Access Control (RBAC) policy that complies with the "Minimum Necessary Requirement."*
		In an effort to minimize administrative overhead, consider establishing a Facility Administrator Role with the necessary privileges to maintain local accounts.
		Ensure that user and facility administrator agreements enumerate responsibilities and expectations, e.g., when an employee no longer needs access to the Newborn Screening Results Portal (NBSRP), NBS program should be immediately notified.
	Identity Proofing Assurance Level	*Automate account provisioning and de-provisioning process.*
		Evaluate vendor options for implementing Remote Identity Proofing (RIDP) as part of account provisioning.
		Consider integrating with the state licensing board as an additional authoritative source for identity verification within NBSRP account provisioning process.
		Establish and implement account lockout policies e.g., inactive account period, expired license, etc.
		Conduct periodic account reviews.
	Self-Service Password Management	*After a predetermined period of inactivity, the NBSRP should automatically logoff the user.*
		For existing NBSRP where possible, work with department IT and vendor in implementing NIST SP 800-63-3 (Digital Identity Guidelines). Evaluate vendor NBSRP solutions for compliance.

Document Section	Category	Recommendation
Report Access and Sharing	**Patient Searches**	*NBS programs should consider who will need access to the NBSRP, what they can access, how they will access it and what options will be available to the user for printing or downloading reports. In particular:* - *What criteria must someone meet to access reports? Only doctors? Other clinic staff who may be assigned to working with patient reports?* - *Who are the intended users? Birthing facilities and hospitals only? Clinics? Other providers as needed?* - *What information will be contained in the system? Result reports only? Case information?* - *Can they access any report once signed in or are they constrained by role or some other criteria (such as facility) as to what information or which patients they can view?* - *Can they access only single reports, or will they have an option to use criteria, such as date collected and facility, to pull a set of reports?* - *How will the user get the reports out of the system? Printing? Downloading?* - *What are the minimum number of identifiers that will be required to search for a record?* - *Will searches require exact information or will the portal allow wildcard searches on partial information for certain fields like name?* - *What are the risks and liabilities for the options chosen?* *NBS programs should involve their IT professionals and someone familiar with privacy practices and state laws when determining the answers to these questions. Circumstances will vary between jurisdictions and there is no universal solution for everyone.*
Transitioning to Use of a Remote Portal	**Communication and Onboarding**	*Develop a robust communication plan for announcing, onboarding and monitoring use of the NBSRP.*
	Staffing	*Model expected staffing needs to oversee and maintain the NBSRP and ensure appropriate coverage to provide high quality customer service.*

Introduction

As newborn screening (NBS) programs continue to move towards establishing electronic access to NBS reports for hospitals, clinics and midwives, the need to establish best practices has become clear. These questions span the gamut from best practices around information technology (IT) to access administration to privacy and authentication practices. The Association of Public Health Laboratories (APHL's) Newborn Screening Technical assistance and Evaluation Program (NewSTEPs) hosted a national *Hot Topic (initiated to provide just-in-time solutions to NBS programs during the COVID-19 pandemic)* webinar on August 12, 2020 that focused on electronic reporting of results, inclusive of web-based reporting portals. During this webinar, numerous questions and concerns were brought up around best practices and the need for guidance on implementing and maintaining report portals.

Scope: This document will only cover web-based report portals, and will not encompass considerations for electronic ordering and reporting using Health Level Seven (HL7) standards. For guidance on electronic ordering and reporting using HL7, see **the Building Blocks: Newborn Screening Health IT Implementation Guide and Toolkit**.

Methods

APHL's Newborn Screening and Genetics (NBSG) program staff reached out to members of the APHL Legal and Legislative Issues in NBS (LLINBS) workgroup and the APHL NBS Health Information Technology (HIT) Interoperability User Group as subject matter experts to assist in the development of the guide. The workgroup that developed this document consists of five members, including APHL NBSG program staff.

The workgroup developed a set of questions that was asked of a convenience sample of NBS programs via video conference. In total six NBS programs were independently interviewed. NBS programs were asked questions covering the following topic areas:

- Systems used
- Functions of the portal, including use cases
- Access to the portal
- User Agreements/Acknowledgments
- Accessing reports
- Audit trails

The questions included:

- What is your program currently doing concerning electronic reporting?
- What are the barriers, solutions, lessons learned?
- Can you share templates of data sharing agreements, screen shots of the reporting system?

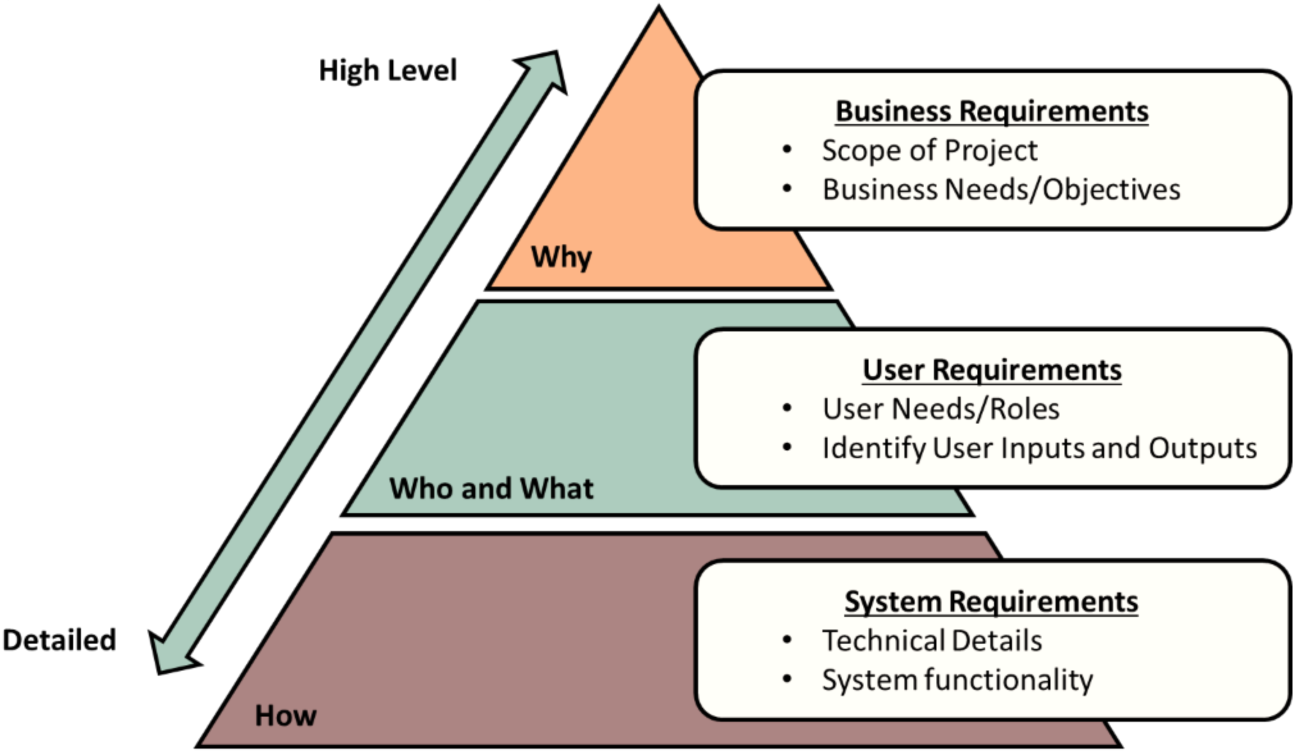
Newborn Screening Results Portals

Requirements and Functionality

Identifying a comprehensive list of requirements and desired functionality is an important first step in moving towards utilization or enhancement of a web-based Newborn Screening Results Portal (NBSRP). Obtaining input from a variety of stakeholders and building several use cases can help ensure that the end product is secure and effective.

Just like any information technology (IT) based project, requirements gathering for a web-based portal involves several stages (Figure 1).

Figure 1: Steps to Requirements Gathering



Step 1: Define the Business Need and Scope (Business Requirements)

Understanding the need to move to a newborn screening results portal (NBSRP) requires full appreciation of the current process for releasing results to various stakeholders. Outlining the current process aids in understanding why a results portal may be needed and how it can help the NBS program reduce staff burden and enhance timeliness. Specific considerations around business needs might include:

- Current number of staff utilized, and time taken, to release and mail NBS reports
- Current number of staff utilized, and time taken, to respond to ad hoc NBS report requests
- Specific requests or feedback from hospital, clinic, or specialty staff

Clearly defining the scope of the NBSRP helps ensure that project objectives are met, and deliverables meet specified needs. By constructing the boundaries of the project, everyone can begin the project on the same page with the same understanding of the desired product.

Step 2: Define the Users and Their Various Needs (User Requirements)

Depending on the identified scope, there may be one or more primary users of an NBSRP. These can include, but are not limited to specimen submitters, midwifery practices, primary care clinics and/or specialists. Once potential users are identified, developing use cases adds value to the management of the project by helping to explain the various users' goals, interactions and subsequent system responses.

Step 3: Define the Technical Details and System Functions (System Requirements)

NBS programs have generally followed one of three approaches for their results portal, each with their own advantages and disadvantages:

1. **Expansion of an existing external-facing agency-wide portal and/or Health Information Exchange (HIE)**
   a. *Advantages:*
      i. Onboarding of new users usually handled at Agency level, reducing burden on NBS staff
      ii. More incentive to utilize the portal as users have access to other important public health information (e.g., immunizations)
   b. *Disadvantages:*
      i. Little flexibility to build NBS-specific processes
      ii. May limit functionality

2. **Utilization of a remote portal solution provided by the NBS program's Laboratory Information Management System (LIMS) vendor**
   a. *Advantages:*
      i. Robust connection to LIMS
      ii. Potential to expand use to provision of and obtaining back follow-up information as well as remote demographic entry within same system
   b. *Disadvantages:*
      i. Onboarding and user management often falls to NBS staff
      ii. Default functionality may be limiting depending on solution offered by LIMS vendor and/or modifications may have additional cost

The following steps have been suggested in writing use cases:[1,2]

1. **Identify** all user groups who will be using the system or portal

2. **Choose** one of the user groups

3. **Define** what that user wants to do in the portal. Each activity the user does in the portal becomes a use case

4. For each use case, **outline** the normal course of events when the user is interacting with the portal

5. Further, **describe** the normal course, including inputs from the user and outputs from the system

6. **Consider** alternate courses of events and add those that may extend the use case (e.g., normally, there is only one specimen, but what happens if there is more than one specimen for a patient?)

7. **Repeat** for all other user groups

3. **In-house development of an NBS-specific remote portal solution**
   a. *Advantages:*
      i. Can customize to NBS program functionality requirements and desires
   b. *Disadvantages:*
      i. May take longer to develop as need to build both connections and user interface

Based on interviews with state NBS programs, features in Table 1 should be considered for remote portal technical system requirements.

Table 1. Newborn Screening Results Portal Requirement Considerations

Feature	Potential Functionality Considerations
Security	• Does the system need to be Health Insurance Portability and Accountability Act (HIPAA)-compliant? • What are password requirements? o Complexity? o Expiration frequency? o Can users reset their own passwords? • Will system be cloud or server-based? • What are authentication and data use agreement requirements upon login?
Development, Testing and Modifications	• Is there a development or test site? • How are modifications made? o Cost? o Timeframe?
Browser and Mobile Compatibility	• Are common browsers compatible with the portal? • Is there mobile compatibility to allow users to retrieve results via mobile platforms?
Down Time and System Recovery	• What is the maximum amount of time the portal can be down? • What are processes for implementing updates to the production site?
Specimen Tracking and Status	• Will users be able to track receipt of specimens? • Will users be able to track pending status of testing?
Report Availability, Formatting, and Timing	• Will preliminary reports be available for actionable results? • What format (e.g., PDF, etc.) will reports be in? • Will additional analyte values (i.e., those not on the report) be available through the portal? • Will search functionality pull up all results for a single patient (e.g., is portal specimen or patient-centered?)
NBS Program Coverage	• Will the system include: o Critical Congenital Health Disease (CCHD) and Early Hearing Detection and Intervention (EHDI) results? o Remote data entry? o Case management/follow-up?
Communication and Notifications	• Can email alerts be sent to users? • Can the landing page be used to provide updates and announcements?

Recommendation: Clearly and concretely describe the business, user and system requirements for the Newborn Screening Results Portal (NBSRP).

Recommendation: Develop a comprehensive list of requirements and desired functionality using input from a variety of stakeholders, including Newborn Screening (NBS) program staff, Information Technology (IT) staff and End-Users.

Data Sharing Agreements

A data sharing agreement is documents the data that is being shared and how it can and cannot be used. It serves both to protect the agency providing the data and to prevent miscommunication between the provider of the data and the organization or individual receiving the data. Since the data from a NBS program contains private health information, the secure storage of the data and the maintenance of that security while it is being accessed, is paramount. The process and language used to design data sharing agreements can vary from NBS program to program depending on the requirements of their parent agency and state. If an online user agreement is used, there should also be a separate application for access in place to identify the specific users prior to them gaining access to the site. Depending on your state, there may already be a data sharing agreement that is available (and often required) for your NBS program to use or you may need to create one from scratch or modify the existing one.

There are many different types of data sharing agreements depending on the requirements of the specific jurisdiction and the intended use. Your jurisdiction may already use one of the common types of agreements below or have a different one that was created to meet specific needs. Some programs may need to use a combination of the data sharing agreements below.

1. **Data Use and Reciprocal Support Agreement (DURSA)** – the DURSA is a comprehensive multi-party agreement that is entered into voluntarily by public and private organizations that want to participate in electronic HIE as part of E-Health exchange. This type of agreement is more applicable to interfacing or other types of electronic HIE.
2. **Memorandum of Understanding (MOU)** – This is a legal document describing an agreement involving two parties where they have a common intent, rather than a legal commitment. It generally lacks the binding power of a contract, depending upon

User agreements can limit liability and define for what purposes users can access the site. Some items that are often included are:

Acceptance of Terms (users agree to adhere to the terms and conditions you/your program set forth)

Acceptable Use (specifies prohibited uses such as data harvesting or the use of data for non-health related purposes)

Modifications of Site (notifies users that you/your program may modify or change the site at any time without notice) and

Support and Maintenance (specifies whether, how and when you/your program will assist users if they have access issues) how it is written. An MOU is distinct from a Memorandum of Agreement (MOA) which is intended to provide a written understanding of the agreement between parties to cooperatively work together to meet an agreed upon objective or accomplish an agreed upon project. It can serve as a legal document or just a partnership agreement.

3. **Interconnection Security Agreement (ISA)** – Once a formal MOA/MOU that defines high-level roles and responsibilities to manage a connection between systems is in place, an ISA may follow. This document is intended to regulate the security interface between two systems operating under two distinct authorities (such as an agency and an external partner) and includes a variety of descriptive, planning, technical and procedural information. This type of agreement would also be most used when performing electronic HIE.
4. **Online User Agreement** – For NBS programs, this may be used as an adjunct to a data sharing agreement and not as the primary data sharing agreement. This is an agreement between the owner, administrator, or provider of a web or mobile application based service and the user of that service. It defines the rights and responsibilities of both the parties. Common examples of this type of agreement include website terms, conditions, and privacy policies. There are two common types of online user agreements: Browserwrap and Clickwrap.
    - A **Browserwrap agreement** is a notice to inform users that by using the site they are subject to terms and conditions. Often there is a hyperlink to the actual terms and conditions. These types of agreements do not require the user to read or accept the terms before using the site and do not offer as much protection as a Clickwrap agreement.
    - A **Clickwrap agreement** requires the user to take some type of action indicating their acceptance of the terms and conditions before using the site (e.g., a box that the user needs to check indicating that they agree to the terms and conditions of use). This type of agreement is far stronger legally than the Browserwrap agreement.

The following are examples of different practices related to data sharing agreements used by the NBS programs interviewed.

1

Case Study

The user agreement is used for all state public health programs access, not just NBS. In this example, an IT staff member receives the data user agreement form and then emails it to the NBS program to approve access.

2

Case Study

There is a document outlining the security parameters needed to share data as well as a facility agreement that is tracked for each facility. There is an agreement for each user that is co-signed by the administrator of their facility. The user access form is available online and completed forms are emailed to the NBS program, where staff manually review them and check the National Provider Identifier (NPI) number against the NPI database. There is an Application Support Group that prompts users to create an account with a secure password in the LIMS and sends email notifications to the user that an account has been set up. In this example, the user access form has gone through legal review before being put into use.

3

Case Study

This NBS program also has the user agreement form online so that it is available. In this case, the Privacy Officer for the Public Health Lab assisted with the development of the user form.

4

Case Study

This NBS program requires that the user's email is associated with a valid license in their database of health professionals. Once the email is validated, they sign the data use agreement and are granted access.

5

Case Study

This NBS program has a state-designated HIE that has a MOU in place with the Department of Health. All facilities have agreements in place with the health information network. The NBS program is currently working with the health information network to include NBS results in their exchange.

6

Case Study

The user agreement is defined by statute and is processed through the legal team. They require an attestation to the agreement each time the user logs in (e.g., a Clickwrap user agreement).

Recommendation: When creating or reviewing the agreement you will use, consider the following items:

- Method of sharing
- Period of agreement
- Intended Use
- Constraints on use
- Data confidentiality
- Data security
- Any legal or other requirements specific to your jurisdiction

Recommendation: Some questions[3] to consider are:

1. What process for authorization is required for people or organizations to access data?
2. Who facilitates the process?
3. Who maintains the process (adds and deletes users, maintains the database and audits it for access and users who should be removed)?
4. Does the agreement for access and use need to be legally binding?
5. Who needs to complete the agreement?
6. Does the person requesting access need authorization and/or verification from their organization?
7. Do they need to meet any specific criteria in order to access data (e.g. have a current medical license)? If so, what are the criteria?
8. In addition to the data sharing agreement to grant access, does the portal need to contain a user agreement that must be agreed to each time the user accesses the site?
9. Are there consequences for misuse of the data and are these consequences clearly stated?
10. How long is authorization good for?
11. Is there a process to remove expired users or those who should no longer have access?
12. What are the requirements for data security?

Table 2. Data Sharing Agreement Considerations

Topic	Potential Access Considerations
Legal	• Does the agreement for access and use need to be legally binding? • Are there consequences for misuse of the data and are they clearly stated? • How long is authorization good for? What are the requirements for data security?
Additional Agreements	In addition to the data sharing agreement to grant access, does the portal need to contain a user agreement that must be agreed to each time the user accesses the site?
Users	• Who needs to complete the agreement? Does the person requesting access need authorization and/or verification from their organization?

Privacy and Security

Cybersecurity Threats

The health care industry has become reliant on the digitization of data and automation of processes to maintain and share patient information and to deliver patient care more efficiently and effectively. In addition, public health departments and health care organizations more broadly have become vulnerable to cyber-attacks on their computer systems and on the data contained therein. These vulnerabilities create significant risks with potential high-impact consequences for health care organizations, their business partners and particularly, their patients. Hackers of all types (nation-state actors, cyber criminals and hacktivists) have found numerous ways to monetize illegally obtained health care data.

Health care organizations require current and resilient cybersecurity that is compatible across organizations without restricting innovative efforts around population health, precision medicine and transparency. Effective cybersecurity is a shared responsibility involving the people, processes and technologies that protect digital data and technology investments. It is a continuous battle as hackers constantly find new ways to defeat cyber-threat defense initiatives, particularly as health care organizations increasingly transmit data electronically, through mobile devices, cloud-based applications, medical devices and technology infrastructures. Some federal initiatives to address these threats follow below.

HIPAA Privacy Rule

The Privacy Rule protects the rights of an individual and their ability to control and access their own protected health information (PHI). [4] Furthermore, it prescribes how medical organizations can use the data for functional activities such as treatment, operations and payment. The Privacy Rule assures that all PHI will be protected from unauthorized disclosure and covers the physical security and confidentiality of PHI in all formats including electronic, paper and oral.

HIPAA Security Rule

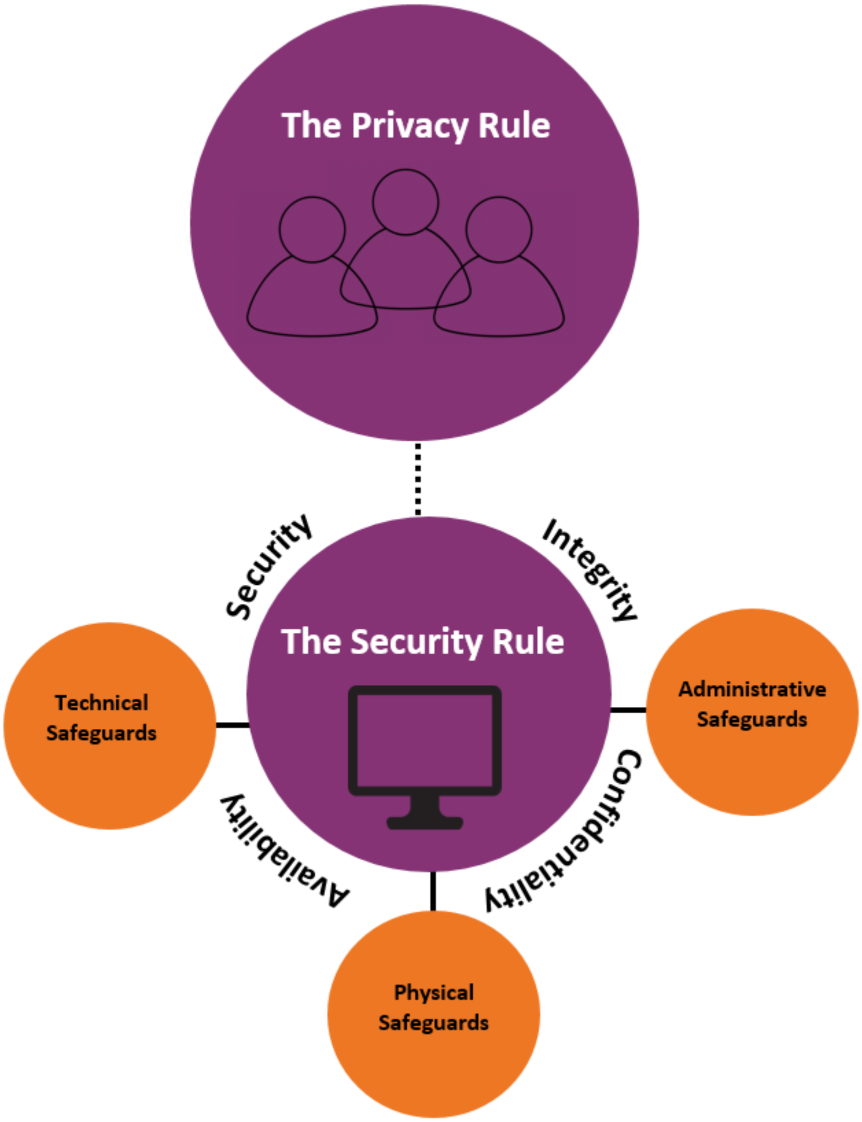
The Security Rule is a subset of the Privacy Rule and is only concerned with the protection of Electronic Protected Health Information (ePHI) that is created, received, or used electronically.[4] Specifically, it protects the security, integrity, confidentiality, and availability of ePHI. The Security Rule requires that covered entities develop internal policies and procedures establishing certain safeguards for the protection of ePHI, including:

- **Administrative Safeguards:** These are the administrative functions that should be implemented to meet the security standards. These include assignment or delegation of security responsibility to an individual and a security training requirement.

- **Physical Safeguards:** These are the mechanisms required to protect electronic systems, equipment and the data they hold from threats, environmental hazards and unauthorized intrusion. They include restricting access to ePHI and retaining off site computer backups.
- **Technical Safeguards*:*** Primarily the automated processes used to protect data and control access to data. They include using authentication controls to verify that the person signing onto a computer is authorized to access that ePHI, or encrypting and decrypting data as it is being stored and/or transmitted, for example, via a NBSRP.

It is important for NBS programs who host a NBSRP to evaluate the effectiveness of these policies and procedures on a periodic basis and to take steps to identify and address threats and vulnerabilities to ePHI security.

Figure 2: The Security Rule:



HIPAA Security Incident

HIPAA requires all covered entities to implement technical controls to safeguard the confidentiality, integrity and availability ePHI. However, even when covered entities have resilient, layered cybersecurity defenses and are fully compliant with HIPAA Security Rule requirements, incidents may still occur as cybersecurity defenses are unlikely to be 100% effective, 100% of the time.

While not all security incidents are considered breaches, the HIPAA Security Rule does provide guidance on security incidents and define them as:

> ***A security incident is an attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. (45 CFR 164.304)***

HIPAA Security Incident Response Plan

When a security incident happens, effective response planning can be a major factor of how significantly a public health department suffers operational or reputational harm. Being able to respond to incidents in a systematic way ensures appropriate response steps are taken each time to help minimize the impact of breaches.

NBS Programs should review the security incident response to make sure the plan was followed correctly and to determine if it can be refined to better meet HIPAA breach notification and HIPAA Security Rule policies and procedures.

Security incident response plans should include procedural details and assignments for how NBS programs will address an incident. The plan should explain how to detect and determine the situation, how to contain the situation, how to correct the situation, and how to recover anything that was affected by the incident. Below are the general phases of a security incident response plan.

1. **Preparation**

   The preparation phase includes steps taken before an incident occurs and typically emphasizes not only establishing an incident response capability, but also preventing incidents by ensuring that systems, networks, and applications remain sufficiently secure. Examples include:

There are many types of security incidents to include:

Malware Attack. A security incident involving any code base attack that can be utilized against a system or network. Designed to attack a system or cause harm to include slowing the system down to include poorly written software with no intent to harm.

Password Attack. This security incident involves hackers using techniques such as Dictionary or Brute Force Attack to comprise user accounts.

Ransomware Attack. Is a special type of malware, which attempts to deny access to a user's data, by encrypting files with a key known only to the hacker. The ransomware directs the user to pay the ransom to the hacker in order to receive a decryption key.

Loss or Theft. Losing an electronic device that contains ePHI, such as an unencrypted laptop or USB device, is a serious security incident that can lead to a major breach.

- **Risk Assessments**. Periodic risk assessments of systems and applications should determine what risks are posed by combinations of threats and vulnerabilities.
- **Vulnerability Assessment**. The process of identifying any weaknesses that may be present in the configuration of computing systems, network appliances and networks. Ensuring configured systems follow the principle of least privilege—granting users only the privileges necessary for performing their authorized tasks.
- **Malware Prevention**. Software to detect and stop malware should be deployed throughout the organization. Malware protection should be deployed at the host level, the application server level, and the application client level.
- **User Awareness and Training**. Users should be made aware of policies and procedures regarding appropriate use of networks, systems, applications and handling PHI/PII. Instruct employees on these policies and procedures, and develop and apply sanctions against employees who do not comply with these policies and procedures. Organizations should train management and staff periodically on the plan, and exercises should be conducted regularly.

2. **Identification**
    - Monitor IT systems and detect deviations from normal operations, and determine if they represent actual security incidents.
    - Incidents may be detected through many different means, with varying levels of detail and fidelity. Automated detection capabilities include network-based and host-based intrusion detection systems, antivirus software, and log analyzers. Incidents may also be detected through manual means, such as problems reported by users.
    - When an incident is discovered, collect additional evidence, establish its type and severity, and document everything.
    - The incident response team should work quickly to analyze and validate each incident, following a pre-defined process and by documenting each step taken.
    - The initial analysis should provide enough information for the team to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident.
    - The incident response team should conduct information impact and/or HIPAA breach risk assessment.
3. **Containment**
    - Perform short-term containment, by isolating the network segment that is under attack, disconnecting the affected system from the network or disabling compromised user account(s).
    - Perform long-term containment, which involves necessary fixes to allow systems to be used in production, while rebuilding clean systems.
    - Prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident.

4. **Mitigation**
   - Remove malware from all affected systems, conduct root cause analysis of the attack, and take action to prevent similar attacks in the future.
   - Eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. Completely wipe and re-image affected system hard drives to ensure any malicious content is removed.
   - Use root cause analysis to further understand what caused the incident. As an example, patching an operating system vulnerability exploited by the attacker.
   - Implement HIPAA technical safeguards (Access Control, Audit Control, Integrity Controls and Transmission Security). For example, updating virus protection software and disabling unused services.
5. **Recovery**
   - Cautiously restoring NBSRP and related systems to normal operation, confirm that the systems are functioning normally, and remediate vulnerabilities to prevent similar incidents where necessary.
   - Provide close monitoring after bringing affected systems e.g., NBSRP back online**.**
6. **Lessons Learned**
   - Document all aspects of an incident in particular while it is ongoing to maintain as comprehensive documentation.
   - Detail ways in which the identification could have occurred sooner and the response could have been quicker or more effective, organizational shortcomings that might have contributed to the incident, and potential areas for improvement.
   - Focus on producing a set of objective and subjective data regarding each incident such as total hours of involvement and the cost, which may be used to justify additional funding of the incident response team.
   - A comprehensive study of incident characteristics may indicate systemic security weaknesses and threats, as well as changes in incident trends.
   - The output from lessons learned can be put back into the risk assessment process, ultimately leading to the implementation of additional administrative, technical, physical controls.

Recommendation: Consider establishing a Cyber Security Incident Response Team (CSIRT) consisting of stakeholders within the NBS program, Laboratory Information Management Systems, Information Security Officer, Privacy Officer, General Counsel and Information Technology Department.

Recommendation: Follow the **National Institute of Standards and Technology (NIST) Special Publication 800-61** Revision 2 “Computer Security Incident Handling Guide” and HIPAA Security Rule policies and procedures when establishing a robust Security Incident Response Plan and establish an initial security incident triage checklist.

Recommendation: Conduct periodic reviews of the security incident response plan as well as practice drills to facilitate effective communication across teams to support coordinated and timely responses help mitigate security incidents.

HIPAA Breach Notification Rule

The HIPAA Breach Notification Rule requires an organization that deals with health information to disclose breaches. The Notification Rule applies to both the Covered Entities (CEs) including healthcare organizations, medical practitioners, insurance companies as well as to the Business Associates (BAs), all of which are organizations or individuals that provide services to the healthcare industry and that have indirect access to PHI. HIPAA defines a breach as:

> ***An impermissible acquisition, access, use, or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of the protected health information. (45 CFR 164.402)***

CEs and their BAs are expected to provide security controls that ensure the confidentiality, integrity, and availability (CIA) of PHI. However, having robust and fairly resilient systems will not eliminate the possibility that a cybersecurity incident could also result in a breach.

HIPAA Breach Risk Assessment

When a breach is suspected, CEs are advised to conduct a risk assessment to determine the probability that the PHI has been accessed by an unauthorized person or persons. This can readily be accomplished as part of the cybersecurity incident response plan. The following factors are to be considered during the assessment:

- **Unintentional Acquisition, Access or Use:** The nature and extent of the PHI involved, including the types of personal identifiers exposed. Assess how identifying the PHI was and if this information makes it possible to re-identify the client or clients involved.
- **Inadvertent Disclosure to Unauthorized Person or Organization**: The identity of the unauthorized person who accessed or used the PHI or to whom the disclosure was made and whether the recipient re-identify the information.
- **Unauthorized Person or Organization Acquire, Retain or View PHI**: Was the PHI actually acquired, retained or viewed?
- **Risk Mitigation**: The extent to which the risk of damage has been mitigated.

HIPAA Breach Exceptions

HIPAA defines the following exceptions to a breach. The following security incidents do not qualify as a breach under HIPAA:

1. Unintentional acquisition, access, or use of PHI by an employee who did so in good faith within the scope of their authority and they do not further disclose the PHI in a manner not permitted by the rule.
2. Inadvertent or accidental disclosure of PHI by an authorized person who shares PHI with another authorized person from the same organization and PHI is not further disclosed in a manner not permitted by the rule.
3. Inability to retain PHI as the organization disclosing PHI is confident the person receiving the information did not have the ability to retain or otherwise compromise the data.

Breach Notification Requirements

The HIPAA Breach Notification Rule outlines three types of entities to be notified in the case of a PHI data breach, individual, media and secretary. Depending on the results of the breach assessment, the covered entity must notify those affected by the breach of unsecured ePHI within 60 days of discovery of the breach. The following are to be notified:

1. **Individuals**
   - You must notify all affected individuals that their PHI was compromised
   - Notification must be performed by first-class mail, or by email if the individual agreed to electronic communication within 60 days of discovering the breach.
   - If you do not have contact details for 1-9 affected individuals, you can use an alternative form of communication like phone, or other written notice.
   - If you do not have contact details for over 10 persons, you may post a prominent notice on your department website's homepage, or on major print or broadcast media in the individuals' place of residence.
2. **Media**
   - Media notification is only required if the breach involves more than 500 individuals in the same state or jurisdiction. In this case, you need to notify the media in that state or jurisdiction, by sending a press release with the same information you sent to the affected individuals in that same area. This must be done within 60 days of discovering the breach.
3. **The Secretary of Health and Human Services**
   - You must also notify the Secretary of Health and Human Services of a breach affecting more than 500 individuals during the same timeframe as you notify the affected individuals. If the breach affected less than 500 individuals, you should maintain an annual breach log, and submit to the secretary within 60 days of the end of the calendar year.

Recommendation: Ensure employees are trained and/or periodically refreshed on HIPAA polices and guidance.

Recommendation: Ensure HIPAA breach response aligns with a documented security incident response plan. This well help establish a clear and well-planned governance to a breach.

Identity and Access Management

Identity and Access Management (IAM) are tools used to manage the roles and access privileges of people and entities to organizational resources. IAM under the HIPAA Security Rule are technical safeguards used in compliance with department security policy. LIMS vendors usually offer an IAM system as part of their NBSRP solution while others may integrate with third party products (e.g., Azure Active Directory).

All IAM systems perform three key functions:

- **Authentication:** The entity is who it claims to be.
- **Authorization:** The entity has the appropriate level of access to resources. Authorization is the process of checking what access the authenticated user is allowed to have to technical resources and ensuring only that access.
- **Audit:** Systematic capture, analysis and response to identity data while proving compliance with regulations, identifying potential security risks and improving security processes.

NBS programs are usually the primary custodians of the provider identities stored in the IAM while the IT department maintains the software and infrastructure. However, overall security ownership is a team effort in collaboration with the NBS program (Lab/Follow-up), IT department, General Counsel and Privacy/Security Officer.

NBS programs with NBSRP hosted by HIE vendors will rely on Business Associate Agreements (BAA), MOUs and/or Service Agreements to establish technical ownership and custodial responsibilities.

5

Case Study

The user agreement is used for all state public health programs access, not just NBS. In this example, an IT staff member receives the data user agreement form and then emails it to the NBS program to approve access.

6

Case Study

This NBS program hosts a LIMS NBSRP solution on premise and has a small IT team and project management to support development efforts. The NBS program also works closely with LIMS consultants and support for maintenance, enhancements and upgrades. The NBS program's IT staff are responsible for managing account provision/de-provisioning, password reset and user authorization setup.

Recommendation: Confirm whether your NBS program is a Health Insurance Portability and Accountability (HIPAA)-covered entity. Although some NBS programs may not be considered covered entities, NBS program leadership should strongly consider following these rules given their adoption within the healthcare industry private sector as best practices.

Recommendation: Define clear procedures for who is responsible for the software maintenance, customer support, technical support, account provisioning/de-provisioning.

Recommendation: Increase security awareness by training NBS program employees on what the rules are and how to abide by them.

Recommendation: Establish a process to review and maintain the policies and procedures to stay up to date and current with the HIPAA Privacy and Security Rules.

User Authentication

While all NBSRP and third party IAM systems implement authentication, usually through a username and a password, the current cybersecurity threats e.g. Ransomware, Spear Phishing, Dictionary attack, Brute Force attack, have demonstrated that username and password are not enough protection for ePHI.[5]

To meet today's more sophisticated cybersecurity threats, the NIST SP 800-63-3 has established Authenticator Assurance Level (AAL) guidance for authentication factors. This guidance should be considered when implementing or selecting a NBSRP solution.

It is imperative that NBSRP improve identity validation by implementing Multifactor Authentication (MFA) which requires more than one authentication factor be presented before the authentication process can be completed: [6,7,8]

- Something you know; e.g., username/password
- Something you have; e.g., cell phone/smart card
- Something you are; e.g., biometric
- Something you do; e.g., repetitive typing pattern
- Somewhere you are; e.g., GPS location/**Internet Protocol** (IP) address

5

Case Study

The NBSRP integrates MFA. As a part of the account provisioning and approval process, the NBS program establishes user identity by requesting among several attributes, the user's cell phone number and username/password. As such, during logon, users enter their username and password ("Something you know"). If successful, the user is subsequently prompted to enter a code sent by the NBSRP to their cell phone ("Something you have").

Recommendation: Implement Multi-Factor Authentication (MFA) such as two-factor authentication: "Something you know" and "Something you have."

Recommendation: When using "Something you have" authentication factor, consider incorporating a mobile authentication application e.g., Microsoft Authenticator and avoid using Short Messaging Service (SMS).

Recommendation: Follow **NIST SP 800-63-3** guidelines for username/password.

Authorization and Role Based Access Control

Role-Based Access Control (RBAC) restricts access based on a person's role within an organization and has become one of the main methods for advanced access control. The roles in RBAC refer to the levels of access that user has within an application.

RBAC is also a common technical control used to implement the "Minimum Necessary Requirement," a key protection in the HIPAA Privacy Rule.[4] The purpose of the requirement is to ensure that organizations give users access to only the **minimum necessary information needed** to perform their work, given their particular role. Minimum necessary requirement is the most effective way to implement RBAC.

NBS programs need to review their NBSRP use cases and consider the minimum access required by users and establish roles accordingly:

- LIMS Staff
- Follow-up
- Hospital, Primary Care Provider
- Specialist, Midwives
- Practice/Facility staff

Consider This:

- *Do hospitals need access to all NBS results or should their access be restricted to only those patients with visits to their facilities?*

Facility Administrator Role

To minimize the administrative overhead associated with maintaining user accounts, NBS programs who host their NBSRP may want to include provisions within their NBSRP agreement whereby they can delegate account maintenance responsibilities to designated proxies with the use of a special role such as Facility Administrator. This role functions as a "proxy" and possesses elevated privileges to activate and deactivate user accounts for a practice/facility.

Most IAM solutions support these capabilities, however, LIMS vendors and/or Third Party (e.g., HIEs) may not. For homegrown NBSRP IAM solutions, such RBAC capabilities may be technically possible and should be prioritized accordingly.

Recommendation: Consider establishing and implementing a robust Role Based Access Control (RBAC) policy that complies with the "Minimum Necessary Requirement."

Recommendation: In an effort to minimize administrative overhead, consider establishing a Facility Administrator Role with the necessary privileges to maintain local accounts.

Recommendation: Ensure that user and facility administrator agreements enumerate responsibilities and expectations; for example, when an employee no longer needs access to the NBSRP, the newborn screening program should be immediately notified.

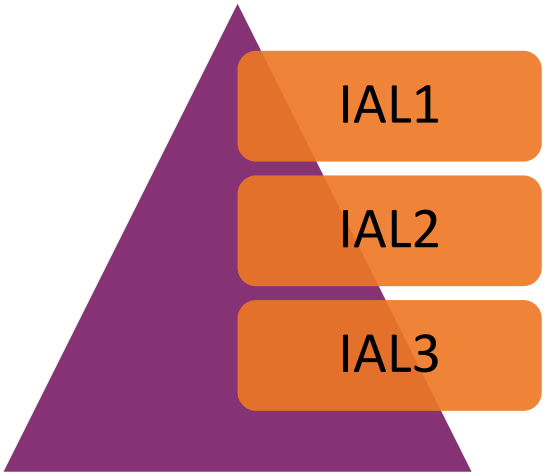
Account Provisioning/De-provisioning

The general process for establishing an NBSRP user account is usually self-registration. The user completes an online request form with information about themselves, their organization and concludes by signing a user agreement. On the NBS program side there may be manual intervention to process submitted PDF forms followed by an identity verification step of the identity attributes e.g., name, license number, etc. Upon successful verification, the user account is activated.

The user identity verification step, also known as Identity Proofing, is the most critical step, the hardest to scale and requires the most administrative overhead as the NBS program must ensure the person applying for access is who they claim to be. A knowledge-based request for a license number is not enough to prevent hackers from impersonating a valid practitioner to access ePHI.[8] In most states, medical license information is publicly available online. Effective identity proofing as a first-line defense against attacks must use Knowledge-Based Verification (KBV) consistent with NIST guidelines

Identity Proofing Assurance Level

NIST published a recommendation known as Special Publication 800-63A Enrollment and Identity Proofing that defines three levels of Identity Assurance: IAL1, IAL2 and IAL3. Each level provides increasing assurance as to the strength of the individual's identity.[9, 10]



IAL1: *There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the authentication process are self-asserted or should be treated as such, including attributes that a Credential Service Provider (CSP) asserts to a results portal.*

IAL2: *Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically present identity proofing. Attributes can be asserted by CSPs to result portals in support of pseudonymous identity with verified attributes.*

IAL3: *Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained representative of the CSP. As with IAL2, attributes can be asserted by CSPs to result portals in support of pseudonymous identity with verified attributes.*

While there are not any specific NBSRP standards, the Department of Health and Human Services (HHS) recommends IAL2 for ePHI interoperability as required by the 21st Century Cures Act.[11] Additionally, a combination of Remote Identity Proofing (RIDP) and MFA meets IAL2, as IAL2 does the following:[9]

- Allows remote or in-person identity proofing
- Supports a wide range of acceptable identity proofing techniques in order to increase user adoption
- Decreases false negatives
- Detects to the best extent possible the presentation of fraudulent identities by a malicious applicant.

US Department of Health and Human Services Case Study

The US Department of Health and Human Services uses RIDP for sites such as the Centers for Medicare & Medicaid Services (CMS) Enterprise Portal. CMS partners with Experian as their external identity verification provider.[8] The account provisioning process starts when CMS Enterprise Portal collects Personally Identifiable Information (PII) such as:

- Full Legal Name
- Social Security Number
- Date of Birth
- Current Residential Address
- Personal Phone Number

These uniquely identifying pieces of information are sent to Experian that verifies the information against their records. As an additional step, Experian may present the applicant with questions based on their credit profile, also called out-of-wallet questions and answers. The information supplied during this exchange is strictly between the applicant and Experian. CMS Enterprise Portal does not store the information.

Recommendation: Automate account provisioning and de-provisioning process.

Recommendation: Evaluate vendor options for implementing Remote Identity Proofing (RIDP) as part of account provisioning.

Recommendation: Consider integrating with the state licensing board as an additional authoritative source for identity verification within NBSRP account provisioning process.

Recommendation: Establish and implement account lockout policies e.g., inactive account period, expired license, etc.

Recommendation: Conduct periodic account reviews.

Password Management

NBSRP are vulnerable to hacker tools capable of cracking passwords in less than 10 minutes using methods such as Dictionary Attack, Phishing attacks and Brute Force attacks. As such, it is important that IAM password management support password policies that make hacking more difficult. The HIPAA Security Rule for Administrator Safeguards, 45 CFR § 164.308(a)(5)(ii)(D) is very vague on password management stating:

> ***"Password Management: Procedures for creating, changing, and safeguarding passwords"***[12]

However, the National Institute of Standards and Technology (NIST) Special Publication 800-63 provides a good foundation for password security guidelines.

Single Sign-On

An NBSRP hosted within their public health department Enterprise Portal (EP) may result in the user having two sets of credentials, which adds more complexity to the user experience. Implementing Single Sign-On (SSO) with Enterprise Identity Management (EIDM) would be an ideal solution as the user can use the same enterprise identity to access multiple web portals within the public health department EP, e.g., NBS, Vital Statistics and Immunizations. One key technical challenge may be that vendor supported NBSRP may not integrate with an EIDM and therefore will not accept the enterprise identity token issued by the EIDM.

Self Service Password Management

To minimize the technical support needed to unlock accounts or reset passwords, an NBSRP should give NBSRP administrators the ability to set user unlock or password reset policies coupled with an additional authentication factor such as mobile One-Time Password (OTP).

Recommendation: After a predetermined period of inactivity, the NBSRP should automatically logoff the user.

Recommendation: For existing NBSRP where possible, work with department IT and vendor in implementing **NIST SP 800-63-3** (Digital Identity Guidelines). Evaluate vendor NBSRP solutions for compliance.

Password Policy and Authentication Enforcement:

- ✓ **8 character minimum** when a set by a human
- ✓ Support at least **64 characters maximum length**
- ✓ Allow at least **10 password attempts** before lockout; the longer and more complex the entry text, the greater the likelihood of user entry errors
- ✓ **No complexity requirements** as users tend to use predictable methods for satisfying these requirements when imposed resulting in weaker passwords and less security
- ✓ **No password expiration period** as users tend to choose weaker memorized secrets when they know that they will have to change them in the near future
- ✓ **No knowledge-based authentication** (e.g., who was your first grade teacher?)
- ✓ **No Short Message Service (SMS) or email for two-factor authentication**; instead use a OTP from a mobile app like Google Authenticator or Microsoft Authenticator

Report Access and Searching

The purpose of a newborn screening results portal is to allow qualified users to access reports for patients in their care. The user must have a way to locate the records they are searching for, and even after authorized login, there must be protections in place to prevent improper access to patient results. In addition to other security, there may also be a need to allow for different levels of access depending on the user's rights or needs for access (i.e., role-based access).

The NBS programs interviewed for this guidance document had different approaches depending on their unique needs, but all identified several different user groups or roles that they considered when developing or implementing their web portal solutions. These included Hospitals/Birth Facilities, Clinics, Providers, Specialists and other NBS programs. Each state had a slightly different approach. Refer to Appendix D: Table 1 – Case Studies.

Once the NBS program has determined who they will allow to access the system, they should also consider how they will allow them to access and interact with the reports.

4

Case Study

This NBS program allows access to only those providers currently licensed in their state. This helps them ensure that only qualified individuals have access and once they do, they are not restricted to whose record they can access (i.e., they have access to all patients regardless of whether the patient is in their care). The benefit of this approach is that the NBS program can maintain security and allow providers to have access to the records for any infant in their care, regardless of who submitted the newborn screen. However, they also identified that they have an issue because military clinicians are not in the state database they use to credential and so these providers cannot currently access records. In addition, the NBS program realizes that in clinics and hospitals it is often not the licensed medical professional who accesses records. Quite often, that task is assigned to a non-medical staff member. Currently their system does not allow non-credentialed personnel to access the NBSRP.

Consider This:

- *The ability to login and obtain results for a single patient is useful, but what about large clinics or hospitals that have multiple births on any given day and need to access reports and print or save them to the file for all the infants born on that day?*
- *Will the NBS program include the functionality to allow a facility representative to search by a date of birth or date of collection and see all reports for a given day? If so, how will the function be limited so that that the user only sees the relevant reports and not others that they do not need and should not have access to?*

NBS programs will need to consider what type of access to records they will allow and weigh the liability versus the benefits of their options. Multi-jurisdictional programs should also consider the need to limit results access to the user's authorized jurisdiction.

Table 3. Results Portal Access and Searching Considerations

Topic	Potential Considerations
Type of access to records	- Weigh the liability versus the benefits of access options provided to users - How will the function be limited to the relevant reports?
Number of Records	- Ability to login and obtain results for a single patient? - Ability to login and obtain results for multiple patients?
Search Criteria	- Allow a facility representative to search by a date of birth or date of collection and see all reports for a given day?

Patient Searches

Matching

One item that needs to be considered when implementing a web portal for results is how the search for records will happen in the background. There are two primary types of matching logic that can be used: Deterministic and Probabilistic.

- **Deterministic matching** can also be referred to as rule-based matching. This type of matching looks for exact matches and does not consider things like spelling variations for last names (e.g. Smith vs Smythe). Due to the nature of this model, data quality can have a large impact on the usefulness of the search.
- **Probabilistic matching** looks for relevant matches based on the fields entered by the user. It uses more complicated algorithms to determine matches, but also better supports things like alternate name spellings.

A hybrid model of the two types of matching can also be used which combines the best features of both.

Patient Search Criteria

Several criteria can be used to perform a search. The most common are listed below and additional examples can be found in Table 2 within Appendix D.

Baby's Last Name

Baby's Date of Birth

Specimen Collection Date

Medical Record Number

Mother's Last Name

Mother's Phone Number

Test Form Number (kit number)

Additional search criteria could include:

- mother’s zip code
- unique laboratory identification number
- gender

The NBS program will need to determine which fields and how many will be required in order to match a record. The more identifiers entered, the more likely it is that the correct record will be found and returned.

Search Errors and How to Prevent Them

If any fields have been incorrectly entered in the system, the search may fail. The fewer fields entered in the search, the more records will be found, but this also increases the possibility that if most of the fields are the same (e.g., in the case of twins or babies with the same last name, date of birth and gender) that an incorrect record could be returned.

NBS programs will need to consider whether the system will display all possible matches and allow the user to make the final determination or whether only exact matches will be returned. It is also possible for information to change between the time of an infant’s birth and when the results are reported. Infants quite often have name changes and this can complicate finding the correct record, especially in two-screen NBS programs where the name may change between the first and second specimen collection.

Many of the NBS programs interviewed use the newborn screening test form number to help definitively identify the infant and prevent search errors. In two-screen NBS programs, the test form number can also be used to link multiple specimens on the same infant so that a complete record is available.

An NBS program may also allow for wildcard searches that can be used to maximize search results. **Wildcards** are used in search terms to represent one or more other characters.

All of these factors should be considered when making the decision about what type of search logic will be used and what identifiers should be present.

Required Minimum Search Parameters

It is important for both patient privacy and data security that users are limited to seeing only what they need to see for the course of their work. Responses from the NBS programs interviewed ranged from requiring one to six identifiers to complete a search.

How the system is set up – whether a user has access to all patients or only those from their facility will also determine how many and which identifiers can be used to perform a search. How the portal will be

Sources of Data Errors

The quality of the data entered in the system can provide additional complications for searching. Sources of data errors may include:

- typographical errors where characters are inserted, deleted or transposed

- phonetic misspellings

Jean vs. Gene

- data entry errors based on letters or numbers that look the same

the number “1” vs “l”

the numbers “1” and “7”

capital letter “I” and lowercase “L”

utilized and the type of security set up (such as role-based access), will help determine the required minimum search parameters to use.

Recommendation: Newborn screening programs should consider who will need access to the NBSRP, what they can access, how they will access it and what options will be available to the user for printing or downloading reports. In particular:

- What criteria must someone meet to access reports? Only doctors? Other clinic staff who may be assigned to working with patient reports?
- Who are the intended users? Birthing facilities and hospitals only? Clinics? Other providers as needed?
- What information will be contained in the system? Result reports only? Case information?
- Can they access any report once signed in or are they constrained by role or some other criteria (such as facility) as to what information or which patients they can view?
- Can they access only single reports, or will they have an option to use criteria, such as date collected and facility, to pull a set of reports?
- How will the user get the reports out of the system? Printing? Downloading?
- What are the minimum number of identifiers that will be required to search for a record?
- Will searches require exact information or will the portal allow wildcard searches on partial information for certain fields like name?
- What are the risks and liabilities for the options chosen?

Recommendation: NBS programs should involve their IT professionals and someone familiar with privacy practices and state laws when determining the answers to these questions. Circumstances will vary between jurisdictions and there is no universal solution for everyone.

Audit Trails and Reports

An audit tra*il* is a record of events and changes. It captures events by logging and recording key information such as who performed an activity, what the activity was, and the time and date it occurred.[13] What is audited will depend on the type of system and the purpose for collecting the information; however, there is certain basic information such as the user (which often includes the IP address), what is accessed, and the date/time that is found in almost every audit trail. Audit trails are useful for several purposes, such as:

- Improving security for data by allowing problems such as illegal access attempts to be spotted
- Showing regulatory compliance with HIPAA and other common regulations
- Gaining insight into who is accessing data and how often
- Trouble-shooting issues
- Managing risk by tracking events, one-off trends and problems and allowing prevention of future recurrences
- Reporting on desired metrics such as result turnaround time, who is accessing the system and how frequently, and other information which can be useful to inform the NBS program

One of the drawbacks of collecting data in an audit trail is that it is only useful if there is staff available to review and analyze it. Simply collecting many data items in the audit trail provides no benefit if the data will never be reviewed.

The following are important items that NBS programs should consider when deciding what information to collect in the audit trail.[14]

- ✓ **Patient Report Access:** Patient reports that have been accessed by a user are important data points to include in your audit log. This is not only important for HIPAA compliance, but also to verify that a user has appropriate access (e.g., can only access records that they should have access rights to view). Rules and regulations governing who can view a patient's record vary from state to state. Some NBS programs allow any provider licensed in their state to grant access to their system to view any patient record, while other NBS programs may restrict access to only the facility or provider who ordered the newborn screen.
- ✓ **Login/Logout Access:** As part of data security, it is important to be able to track who accessed the system, when and how long they were in the system. Recording failed logins will also help detect an unauthorized user trying to gain access or a user that is having trouble with access. Including this information in the audit trail will allow monitoring of unsuccessful log in attempts and how often this occurs, which can be important both from a security standpoint as well as for assisting users that may be having issues.
- ✓ **Patient Search Hit/Miss Ratio:** To make it easy for providers to find patient results, it is necessary to develop and run patient search reports that can

be used to determine the performance of patient searches such as response time, match frequency and commonly used search parameters.

- ✓ **Inactive Accounts:** By collecting data on who is using the system and how often, the audit trail allows the administrator to determine which accounts have become inactive and need to be archived or deleted from the system. This helps with security as well as allowing the database of users to remain streamlined.
- ✓ **Product Improvement:** The audit trail is also a useful tool for providing data when issues are reported or enhancements are requested. By keeping a chronological log of activity, the administrator can pinpoint and troubleshoot issues that are reported as well as monitor changes or fixes to the programming.

Transitioning to use of a Remote Portal

Communication and Onboarding

As with any new initiative in newborn screening, communication to relevant stakeholders is key. This is especially true when the initiative is likely to alter existing end-user workflows.

Development of a communication plan for rolling out a new or enhanced NBSRP can improve uptake and buy-in, promote a better user experience and ensure a smoother transition. In general, the communication plan should include three phases and may benefit from components of **Organizational Change Management** (OCM).

Phase 1: Announcing

WHEN: This phase should be initiated well in advance (several months) of going live with the NBSRP.

PURPOSE: The purpose of this phase is to alert stakeholders that this change is coming and to provide enough time for end-users to consider what workflow changes may be needed.

MESSAGING: Messaging during this phase should discuss why the NBS program is moving to a NBSRP and how use of this portal will benefit end-users (e.g., decreased time, burden, increased access, etc.). Concerns or questions from stakeholders should also be solicited during this time.

MODALITY: Announcements to end-users may be accomplished through mailed letters, email listservs, website notifications, within quality assurance reports or when sending out collection devices/NBS kits.

Phase 2: Onboarding

WHEN: This phase should be initiated shortly (weeks) before the Go Live date.

PURPOSE: The purpose of this phase is to train stakeholders to use the portal and provide a walk-through of processes/user guide. It also includes developing a process for and obtaining immediate feedback from stakeholders upon initial use and/or viewing of the system.

MESSAGING: Messaging during this phase should provide clear guidance on how the user will access and interact with the NBSRP as well as a solicitation for feedback on utility of the NBSRP and areas needing improvement. Clarification on which results (e.g., all results after X date) will be available in the NBSRP should be made, and the process for obtaining older or other results not in the NBSRP should be communicated.

MODALITY: Training and feedback can be done in a variety of ways. These include online or paper User Guides and Training Manuals, hosting webinars or through emailed instructions. Any training should also be available in the NBSRP itself or on the NBSRP website.

Phase 3: Monitoring

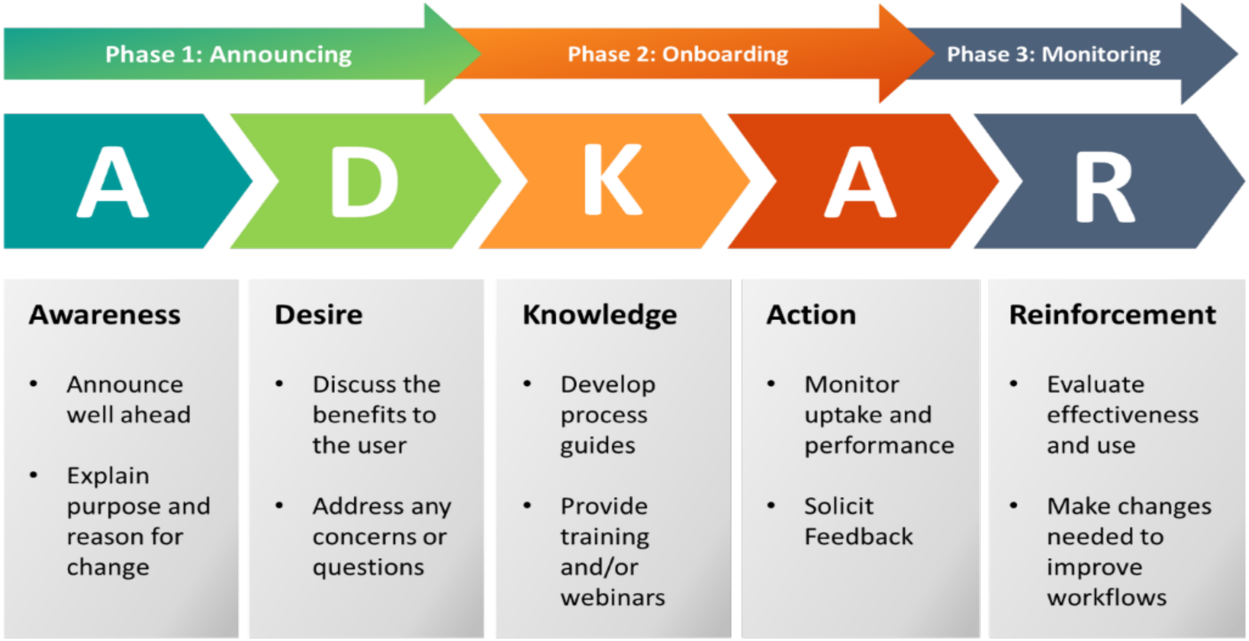
WHEN: This phase should be initiated at a defined time after the Go Live date and continued at regular intervals thereafter.

PURPOSE: The purpose of this phase is to monitor uptake and ongoing use of the NBSRP. It serves to assess ongoing utility and determine if any changes are needed.

MESSAGING: Messaging during this phase should be focused on continued use of the NBSRP as well as solicitation of ongoing feedback or other potential needs within the NBSRP.

MODALITY: Ongoing feedback regarding the NBSRP can be solicited via email or through the NBSRP itself. NBS programs may consider issuing a brief survey to users on a periodic basis.

Figure 3: The diagram below further outlines key communication plan and OCM components.



Awareness

- Announce well ahead
- Explain purpose and reason for change

Desire

- Discuss the benefits to the user
- Address any concerns or questions

Knowledge

- Develop process guides
- Provide training and/or webinars

Action

- Monitor uptake and performance
- Solicit Feedback

Reinforcement

- Evaluate effectiveness and use
- Make changes needed to improve workflows

Recommendation: Develop a robust communication plan for announcing, onboarding and monitoring use of the NBSRP

Staffing

NBS programs should thoroughly understand staffing needs during the onboarding and monitoring phases of the project. Staff needs will depend heavily on the following components:

1. Onboarding and training plans
2. User identification and authentication processes (see the **Privacy and Security: User Authentication Section**)
3. Password management requirements (see the **Privacy and Security: Password Management Section**)

NBS programs should work with their IT team to understand roles and responsibilities and assure that coverage exists to provide high-quality customer service and the ability to onboard new users in a timely manner. Consideration of weekend needs should also be explored, and coverage should be determined for non-business hour needs.

Recommendation: Model expected staffing needs to oversee and maintain the Newborn Screening Results Portal, and ensure appropriate coverage to provide high quality customer service.

Future Directions

The recommendations in this document will help ensure that NBS programs are utilizing best practices in developing and maintaining their NBSRP. In addition, NBS programs have reported delays in implementation of these systems due to not having a clear understanding of authentication and administration requirements. This guidance document will help NBS programs move forward more quickly and enhance implementation. APHL will continue to collaborate with and support NBS programs in these efforts.

List of Acronyms

AAL	Authenticator Assurance Level
APHL	Association of Public Health Laboratories
BAA	Business Associate Agreement
CCHD	Critical Congenital Heart Disease
CMS	Centers for Medicare & Medicaid Services
CSP	Credential Service Provider
DOB	Date of Birth
DURSA	Data Use and Reciprocal Support Agreement
EHDI	Early Hearing Detection and Intervention
EIDM	Enterprise Identity Management
EP	Enterprise Portal
ePHI	Electronic Protected Health Information
HHS	Health and Human Services
HIE	Health Information Exchange
HIT	Health Information Technology
HIPAA	Health Insurance Portability and Accountability Act
HRSA	Health Resources and Services Administration
IAM	Identity and Access Management
IP	Internet Protocol
ISA	Interconnection Security Agreement
IT	Information Technology
KBV	Knowledge-Based Verification
LIMS	Laboratory Information Management System
LLINBS	Legal and Legislative Issues in Newborn Screening
MFA	Multi-Factor Authentication
MOA	Memorandum of Agreement

MOU	Memorandum of Understanding
NBS	Newborn Screening
NBSG	Newborn Screening and Genetics
NBSRP	Newborn Screening Results Portal
NewSTEPs	Newborn Screening Technical assistance and Evaluation Program
NPI	National Provider Identifier
NIST	National Institute of Standards and Technology
OCM	Organizational Change Management
OTP	One-Time Password
PCP	Primary Care Provider
PHI	Protected Health Information
PII	Personally Identifiable Information
RBAC	Role Based Access Control
RIDP	Remote Identity Proofing
SMS	Short Messaging Service
SSO	Single Sign-On
USB	Universal Serial Bus

Glossary of Terms

Acceptance of Terms users agree to adhere to the terms and conditions you/your program set forth

Acceptable Use specifies prohibited uses such as data harvesting or the use of data for non-health related purposes

Administrative Safeguards administrative functions that should be implemented to meet the security standards

Audit Trail a record of events and changes

Browserwrap Agreement a notice to inform users that by using the site they are subject to terms and conditions

Brute Force Attack using trial-and-error to guess login info, encryption keys, or find a hidden web page

Clickwrap Agreement requires the user to take some type of action indicating their acceptance of the terms and conditions before using the site

Data Sharing Agreement a contract that documents the data that is being shared and how it can and cannot be used

Data Use and Reciprocal Support Agreement a comprehensive multi-party agreement that is entered into voluntarily by public and private organizations that want to participate in electronic health information exchange as part of E-Health exchange

Deterministic Matching looks for exact matches and does not consider things like spelling variations

Dictionary Attack an attempted illegal entry to a computer system that uses a dictionary headword list to generate possible passwords

Enterprise Identity Management a framework of policies and technologies for ensuring that the proper people in an enterprise have the appropriate access to technology resources

Enterprise Portal a framework for integrating information, people and processes across organizational boundaries in a manner similar to the more general web portals

Facility Administrator functions as a “proxy” and possesses elevated privileges to activate and deactivate user accounts for their practice/facility

Identity and Access Management tools used to manage the roles and access privileges of people and entities to organizational resources

Identity Proofing an identity verification step of the identity attributes e.g., name, license number etc.

Internet Protocol a set of rules governing the format of data sent over the Internet or other network

Interconnection Security Agreement a document intended to regulate the security interface between two systems operating under two distinct authorities

IP Address a unique string of characters that identifies each computer using the Internet Protocol to communicate over a network

Knowledge-Based Verification a method of authentication which seeks to prove the identity of someone accessing a service

Memorandum of Understanding a legal document describing an agreement involving two parties where they have a common intent, rather than a legal commitment

Minimum Necessary Requirement ensures organizations give users access to only the minimum necessary information needed to perform their work, given their particular role

Modifications of Site notifies users that you/your program may modify or change the site at any time without notice

Multi-Factor Authentication a security mechanism in which individuals are authenticated through more than one required security and validation procedure

One-Time Password a password that is valid for only one login session or transaction, on a computer system or other digital device

Online User Agreement an agreement between the owner, administrator, or provider of a web or mobile application based service and the user of that service

On-Premise Software software that is installed and runs on computers on the premises of the person or organization using the software, rather than at a remote facility such as a server farm or cloud

Organizational Change Management a framework structured around the changing needs and capabilities of an organization

Privacy Rule protects the rights of an individual and their ability to control and access their own protected health information

Probabilistic Matching looks for relevant matches based on the fields entered by the user

Physical Safeguards the mechanisms required to protect electronic systems, equipment and the data they hold, from threats, environmental hazards and unauthorized intrusion

Ransomware a type of malicious software designed to block access to a computer system until a sum of money is paid

Remote Identity Proofing used when the user is not expected to present themselves or their documents at a physical location

Role Based Access Control restricts access based on a person's role within an organization

Security Rule a subset of the Privacy Rule and is only concerned with the protection of Electronic Protected Health Information (ePHI) that is created, received, or used electronically

Single Sign-On an authentication process that allows a user to access multiple applications with one set of login credentials

Spear Phishing the fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information

Support and Maintenance specifies whether, how and when you/your program will assist users if they have access issues

Technical Safeguards the automated processes used to protect data and control access to data

Wildcards used in search terms to represent one or more other characters

List of Appendices

Appendix A: Examples of Data Use and Sharing Agreements

1. Web Portal Request Form for the State Hygienic Laboratory
2. IT Security Requirements

Appendix B: Examples of Training/Onboarding Materials

1. OpenELIS Web Portal User Guide
2. How to Access Neonatal Screening (INMSP) Test Results on the Iowa State Hygienic Laboratory Website

Appendix C: Case Studies

Case Studies for Report Access

Table 1: Access by Role

Case Study Number	Hospitals	Clinics	Specialists/Providers	Other Programs
1	The facility takes the responsibility for printing out the report. They can filter by date range and limit the search using multiple fields such as name, date of birth (DOB) and collection date. They can also use a release date or hospital provided medical record number to generate a report	Primary clinics do not have access to the reports – hope to have this in the future • Challenges include manpower to manage users and the authority to do this • Authorization workflows still need to be worked e.g., the State will be responsible for primary care provider (PCP) verification and access	Can see everything that follow-up sees right now • Results for all states, that come in under queues • Has state and facility ID, PCP name, contacts list • See a snap shot of patient demographics • See results for screen (tabs for each screen) • Can see numerical results • Place to document notes on who was talked to, time and date. Right now this is free text, want to get to a minimum list of outcomes Specialists reportedly hardly log in now – follow-up sends that email with this info already • Currently send via secure email – not convenient and the emails are not available after 2 weeks	Have given access to other NBS programs via the department of health • To follow those babies that move to other states • States must sign agreements to access the data

Case Study Number	Hospitals	Clinics	Specialists/Providers	Other Programs
			○ Typically use name and DOB to search based on email ○ State program coordinators – are not able to filter by facility ○ Will be available in new system	
2	Users have to periodically review the portal for results • There is no automatic push/alert to notify users that a report is complete Would be an ideal feature to have	2 – screen state • PCPs wants results as well • PCPs not necessarily associated with the birthing facility • Have a check box to search all specimens – application enforces a combo of entries so that the record to be returned ○ Has to be an exact match – which is a good control but limits the provider to know the parameters on both specimens and the data in the database needs to have all the parameters entered	Specialists considered as providers • Do have access but not streamlined • Any individual provider can get an account but would need to be associated with a submitter ID • Can call follow-up program for the information	N/A

Case Study Number	Hospitals	Clinics	Specialists/Providers	Other Programs
3	Providers log in to search for baby using 6 pieces of demographics to search on • Form number is used to access results • Can search this number and get report • If no number: last name of baby, last name of mother, DOB, hospital of birth, medical record number • Working on having facilities download reports by facility • Still send out paper reports • If hospitals have a log in and feel comfortable routinely getting their reports electronically; will stop the paper reports Ideally would like a pop-up window with high-level results even if the report is not complete and printed out • Can see specimen has been received and is being tested	Providers (including midwives, if have signed up) log in to search for baby using 6 pieces of demographics to search on • Form number is used to access results • Can search this number and get report • If no number: last name of baby, last name of mother, DOB, hospital of birth, medical record number	Follow-up does not utilize portal so specialists rarely access.	N/A

Case Study Number	Hospitals	Clinics	Specialists/Providers	Other Programs
4	Identified Limitations: Military bases, and physicians outside state cannot access since they are not licensed in state. Looking into how these users can access portal	Provider based access	Provider based access	N/A
5	Have ability to do remote data entry	Can search on a number of demographics (at least 3 pieces) – not tied to a facility, as long as they have the baby's information		N/A

Case Studies for Report Search Criteria

Table 2: Search Parameters

Case Study Number	Who has access	Comments on Matching	Search Criteria	Minimum Parameters
1	Hospitals, Hospital Providers, Other NBS programs		Name, DOB, Collection Date. Can put in multiple fields to limit search	3
2	Hospitals, Clinics, Providers	Search parameters depend on what facility a specimen was collected	DOB, Form number, Baby first and last name, Mother first and last name, Date collected, Medicaid number, medical record number, NBS ID, submitter name, physician name, mother's maiden name, mother's SSN, Lab number, mother phone number	1
3	Hospitals, Clinics, Providers	Would like more fields to search on, would like to be able to do wildcard search on partial last name	Require 6 fields or can use form number last name of baby, last name of mother, DOB, hospital of birth, medical record number	6 or Form Number
4	Hospitals, Clinics, Providers	Require minimum 2 characters for last name	Minimum of 4 criteria: • Form number • First name • Last name • DOB • Gender	4
5	Hospitals, Clinics, Providers		Search on at least 3 identifiers: • Form Number • DOB • Last name • First name • Mom's Last Name	

Case Study Number	Who has access	Comments on Matching	Search Criteria	Minimum Parameters
			- Mom's Phone Number	
6		Can do wild type searches using first few letters of last name	Only have to use one identifier: - DOB - Birth Hospital - Form Number Mother's First Name - Mother's Last Name	

References

[1] Randolph, Gary. Use-Cases and Personas: A Case Study in Light-Weight User Interaction Design for Small Development Projects. *Informing Science: The International Journal of an Emerging Transdiscipline*. 2004; 7. 10.28945/505.

[2] U.S. General Services Administration website. Use Cases. https://www.usability.gov/how-to-and-tools/methods/use-cases.html. Published October 9, 2013. Accessed June 21, 2021.

[3] Commonwealth of Australia, Department of the Prime Minister and Cabinet website. Best Practice Guide to Applying Data Sharing Principles. https://pmc.gov.au/sites/default/files/publications/data-sharing-principles-best-practice-guide-15-mar-2019_0.pdf. Published March 15, 2019. Accessed June 21, 2021.

[4] U.S. Department of Health and Human Services website. The HIPAA Privacy Rule. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html. Published December 10, 2020. Accessed June 21, 2021.

[5] Fu K, Sit E, Smith K, Feamster N. Dos and Don'ts of Client Authentication on the Web. Proceedings of the 10th USENIX Security Symposium, Washington, D.C., August, 2001. https://pdos.csail.mit.edu/papers/webauth:tr.pdf. Accessed June 21, 2021.

[6] Davis J. Best Practice Cybersecurity Methods for Remote Care, Patient Portals. HealthITSecurity. https://healthitsecurity.com/news/best-practice-cybersecurity-methods-for-remote-care-patient-portals. Published April 24, 2020. Accessed June 21, 2021.

[7] Van Wagenen J. The Benefits of Multifactor Authentication in Healthcare. HealthTech. https://healthtechmagazine.net/article/2018/12/benefits-multifactor-authentication-healthcare-perfcon. Published September 24, 2020. Accessed June 21, 2021.

[8] Centers for Medicare and Medicaid Services website. Questions and Answers about Remote Identity Proofing and Multi-Factor Authentication. https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/Downloads/HETSHPGRIDPMFAFAQ.pdf. Published October 2015. Accessed June 21, 2021.

[9] Healthcare Information and Management Systems Society website. HIMSS Identity Management Task Force. Patient Portal Identity Proofing and Authentication. http://s3.amazonaws.com/rdcms-himss/files/production/public/Patient_Portal_Identity_Proofing_and_Authentication_Final.pdf. Published 2016. Accessed June 21, 2021.

[10] Grassi PA, Fenton JL, Lefkovitz NB, et al. Digital Identity Guidelines Enrollment and Identity Proofing Requirements. *NIST Special Publication 800-63A*. https://pages.nist.gov/800-63-3/sp800-63a.html. Published June 2017. Accessed June 21, 2021.

[11] U.S. Food and Drug Administration website. 21st Century Cures Act. https://www.fda.gov/regulatory-information/selected-amendments-fdc-act/21st-century-cures-act. Published January 31, 2020. Accessed June 21, 2021.

[12] Department of Health and Human Services website. HIPPA Security Series. 2:1-29. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf. Revised March 2007. Accessed June 21, 2021.

[13] National Research Council (US) Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure. For the Record Protecting Electronic Health Information. Washington (DC): National Academies Press (US); 1997. Available from: https://www.ncbi.nlm.nih.gov/books/NBK233429/ doi: 10.17226/5595. Accessed June 21, 2021.

[14] American Immunization Registry Association website. Security Guidance Considerations for Immunization Information Systems. https://repository.immregistries.org/files/resources/595e4e25ab1b1/aira_security_guidance_-_final_new_logo.pdf. Published June 2017. Accessed June 21, 2021.