NHSN
NATIONAL HEALTHCARE SAFETY NETWORK

July 2025

NHSNLink:
Architecture and Information Assurance Overview

NHSNLink Background

NHSNLink is an open-source application developed by Lantana Consulting Group for the Centers for Disease Control and Prevention (CDC). NHSNLink uses Health Level Seven International® (HL7) Fast Healthcare Interoperability Resources® (FHIR) to enable reporting of FHIR digital quality measures (dQMs) for surveillance of public health and patient-safety events via the National Healthcare Safety Network (NHSN). NHSNLink is installed within the CDC firewall and allows NHSN to connect securely to a healthcare facility's EHR via the FHIR application programming interface (API), extract and evaluate patient-level data, and submit it to NHSN for analysis.

The NHSNLink application can perform the following actions:

- Configure a facility for reporting dQMs to NHSN according to the HL7 NHSN dQM Reporting Implementation Guide
- Connect to facility data sources, including EHR FHIR APIs
- Identify patients of interest
- Acquire necessary data from facility data sources
- Clean and transform data into a standard form
- Evaluate data for identified patients of interest for configured dQM(s)
- Validate data against the HL7 NHSN dQM Reporting Implementation Guide
- Submit FHIR MeasureReport data to NHSN

NHSNLink Architecture and Operational Process

NHSNLink's architecture allows for horizontal, elastic scalability to respond to external system demand (e.g., data transfer and computational load).

NHSNLink integrates with CDC information security systems and facility systems for security and data governance compliance. It has robust capability to track data provenance and transformation that can be used for audit and incident response activities.

The design, development, and implementation of NHSNLink follow secure coding policies in compliance with the Federal Information Security Modernization Act (FISMA),[i] aligned with CDC security requirements for a system to obtain an Authority to Operate (ATO) via their System Assessment and Authorization (SA&A) processes.

Data within NHSNLink (as with all NHSN systems) are protected by administrative, technical, and physical security controls that safeguard the confidentiality, integrity, and privacy of personal information according to industry-standard policies and federal laws, including FISMA, the Privacy Act of 1974,[ii] and the Health Insurance Portability and Accountability Act (HIPAA).[iii]

The security architecture of NHSNLink is reflected in the following specifications, shown in Figure 1:

- NHSNLink follows National Institute of Standards and Technology (NIST) 800-63 identity guidelines.[iv] Input and output are protected by an OAuth2.0 implementation with OpenID Connect-compliant identity provider for connection to facility data systems and NHSN endpoints.
- NHSNLink is protected by an OAuth2.0 identity-access management (IAM) service delivered by CDC Secure Access Management Services (SAMS), which includes authentication and role-based access control (RBAC).
- NHSNLink queries are for prespecified FHIR resources that are available only upon authorization from the facility's server. The facility can authorize NHSNLink's access to each resource type, thereby controlling which resources are pulled.
- NHSNLink data (including internal NHSNLink app communications) are encrypted in-transit through HTTPS/TLS1.3+.
- NHSNLink data are encrypted at-rest using NIST Advanced Encryption Standard 256 (AES 256)[v] implementation.

NHSNLink PHI/PII Data Acquisition

Participation in the NHSNCoLab is governed by the participating facilities' signed agreements of the following documents, which outline the framework for Protected Health Information (PHI) and Personally Identifiable Information (PII) data acquisition:

- *National Healthcare Safety Network Agreement to Participate and Consent*[vi]
- *National Healthcare Safety Network Facility/Group User & Administrator Rules of Behavior*[vii]

Data retention is subject to NHSN policy.

NHSNLink Data Security and Privacy

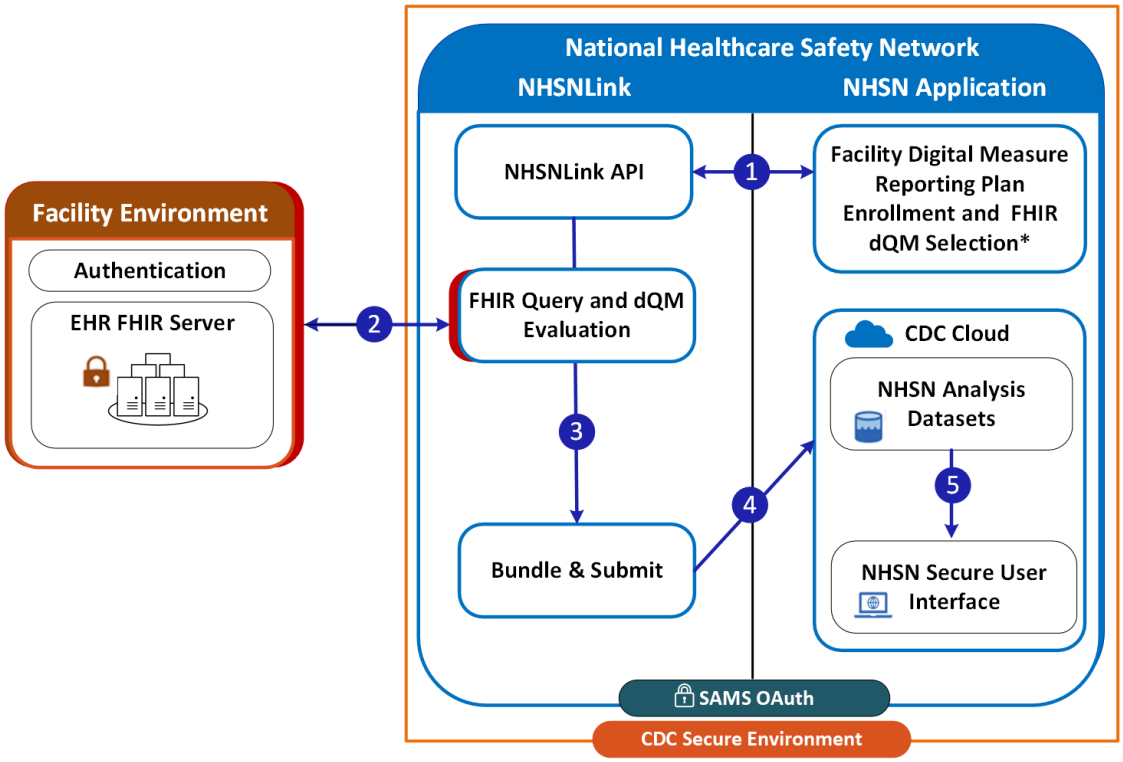
- Within CDC, user access to PHI, PII, and Sensitive PII (SPII) is restricted in accordance with the NIST control AC-06 principle of least privilege.
- Data are classified as FIPS-199 Moderate impact.
- NHSNLink follows the NIST access control (AC) family:
    - AC-01 Access Control Policy and Procedures

- AC-02 Account Management
  - Disable Inactive Accounts and Sessions
  - Automated Audit Actions
- AC-03 Access Enforcement with PII/PHI
- AC-04 Information Flow Enforcement
- AC-05 Compartmentalization with Separation of Duties/Concerns
- AC-06 Least Privilege including restricted access to PII/PHI.

Incident Response (IR)

- NHSNLink operates under the *Memorandum for Heads of Executive Departments and Agencies, Preparing for and Responding to a Breach of Personally Identifiable Information.*[viii]
- The *United States Department of Health and Human Services (HHS) Policy for Preparing and Responding to a Breach of Personally Identifiable Information*[ix] addresses the Office of Management and Budget (OMB) Memorandum outlining the HHS approach in preparing and responding to breaches of PII.

Figure 1. How NHSNLink Works



*Signals facility is ready to report digital quality measure and has signed NHSN data-use agreements for secure data-sharing.

1. Confirm facility enrollment in digital measure reporting plan; request and receive NHSN FHIR dQM
2. Request and receive patients of interest and query data defined by dQM
3. Evaluate and filter data as defined by dQM
4. Submit MeasureReport Bundle for patients meeting dQM definition
5. NHSN ingests and analyzes MeasureReport Bundles and makes reports available via secure NHSN user interface

References

[i] Cybersecurity and Infrastructure Security Agency. *Federal Information Security Modernization Act*. https://www.cisa.gov/federal-information-security-modernization-act (accessed November 2022)
[ii] U.S. Department of Health and Human Services. *The Privacy Act.* https://www.hhs.gov/foia/privacy/index.html (Accessed November 2022)
[iii] U.S. Department of Health and Human Services. *Health Information Privacy*. https://www.hhs.gov/hipaa/index.html (Accessed November 2022)
[iv] National Institute for Standards and Technology. *NIST SP 800-63 Digital Identity Guidelines*. https://pages.nist.gov/800-63-3/ (Accessed November 2022)
[v] National Institute for Standards and Technology. FIPS 197: Advanced Encryption Standard. https://csrc.nist.gov/publications/detail/fips/197/final (Accessed November 2022)
[vi] *National Healthcare Safety Network Agreement to Participate and Consent.* This document can be supplied by NHSN upon request.
[vii] National Healthcare Safety Network. *National Healthcare Safety Network Facility/Group User & Administrator Rules of Behavior.* http://www.cdc.gov/nhsn/PDFs/FacAdminROB.pdf (accessed April 2022)
[viii] Office of Management and Budget. *Memorandum for Heads of Executive Departments and Agencies, Preparing for and Responding to a Breach of Personally Identifiable Information.* https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf (Accessed November 2022)
[ix] U.S. Department of Health and Human Services. *HHS Policy for Preparing for and Responding to a Breach of Personally Identifiable Information (PII)*. https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/hhs-policy-preparing-and-responding-breach.html (Accessed November 2022)