Annual Surveillance Plan
CY 2022

Prepared by: Drummond Group

Questions: surveillance@drummondgroup.com
Phone: 925-235-9344 Karen Stewart

Table of Contents

Introduction and Overview

Surveillance is a central component of the Office of the National Coordinator (ONC) Health IT Certification Program, and its general direction comes largely from three parts. As part of its accreditation to the certification body standard ISO 17065, Drummond Group is required to follow certain tenets of surveillance directed by this guideline. Also, the ONC issues annual surveillance guidance for its Authorized Certification Bodies (ACBs). Finally, ONC federal regulations, most recently the 2015 Edition Final Rule, dictate explicit surveillance requirements.

The Drummond Group 2022 Surveillance Plan for certified Health IT is directed by all three aspects, and it is intended to implement a consistent, thorough and fair policy of surveillance of certified Health IT modules so that all stakeholders, including ONC, vendors, providers and patients have confidence Health IT applications are working as intended.

Drummond Group Approach for 2022 Surveillance

The approach for surveillance in 2022 is divided into two broad categories: Drummond-initiated proactive surveillance and non-Drummond-initiated reactive surveillance.

Proactive surveillance includes, re-testing based on developer attestations, mandatory disclosure requirements, API Documentation requirements and appropriate use of the ONC Certification Mark.

Reactive surveillance comes from receiving complaints or other information about certified Health IT systems which lead to decisions to investigate compliance to the certification requirements or the adequacy the developer's user complaint process. Reactive surveillance is also triggered after multiple requests for certification inheritance on a certified product.

Commitment to Surveillance

Drummond Group considers quality surveillance a vital part of its organization and certification policy. Surveillance ensures confidence that Drummond Certified™ products continue to comply with the criteria to which they were certified. Drummond Group has a Surveillance Program Manager dedicated to overseeing the surveillance activities. The Surveillance Program Manager reports surveillance activity directly to the Drummond Group Certification Body and has access to executive management. The surveillance effort of Drummond Group's ACB is closely monitored by the ONC and ANSI to ensure that products are maintaining their certification over time.

Drummond Group holds regular surveillance committee meetings to review the status of surveillance activities in accordance with Drummond's Annual Surveillance Plan. In addition, the quarterly executive-level Management Review Meeting of the certification body actions reviews the surveillance efforts, complaints in process, status on website reviews, etc.

Drummond Group is also committed to transparency and to fairness in how surveillance is applied and demonstrated. On the Drummond Group website, both this Surveillance Plan and the EHR Certification Guide are published and clearly communicate plans for surveillance. For complaints, please contact us at ehrcomplaints@drummondgroup.com.

Initial Certification: Start of Surveillance

Though surveillance is inherently focused on activities outside of the controlled environment, the process begins after controlled lab environment testing is done and the certification is initiated. Key documents are collected before issuing certification and then used in the surveillance process. Before certifying with Drummond Group, each developer must submit documentation for the Complaint Certification Information Review, and Certification Disclosures. As part of the quality checking process, certification is granted only when all required documents have been submitted successfully.

MSA and Contractual Obligations

For every certification, the developer customer signs a Drummond Group Master Services Agreement (MSA) that includes a surveillance section requiring a variety of items related to surveillance activities. The MSA will require provision of the developer's customer list to Drummond Group as needed for conducting surveillance activities. MSA and Statements of Work (SOW) will identify any costs associated with surveillance activities.

Complaint Certification Information Review

A **Complaint Certification Information Review** (CCIR) form outlines the developer's process for handling complaints from customers. This process must give extra attention to the prioritized surveillance criteria, especially the safety related capabilities. The CCIR form is reviewed by the Certification Body to ensure it satisfies the ISO 17065 standard. The CCIR form is kept on file for the developer and referenced during various surveillance activities.

Conditions and Maintenance of Certification

The 21st Century Cures Act requires that health IT developers conspicuously post on their website a mandatory disclosure of costs for their certified product(s). The following disclosure information will be collected from vendors prior to issuing a certification:

- Additional types of costs or fees that a user may be required to pay to purchase, license, implement, maintain, update, use or otherwise enable and support the Health IT Module's capabilities.

Drummond Group provides instructions and guidelines to assist developers in accurately completing these requirements.

The hyperlink to the disclosure information on the developer's website for each certified product is reported on the CHPL. Thus, the developer must submit this hyperlink prior to receiving certification. The developer is provided a small grace period after certification to make additional modifications to their disclosure language per Drummond Group request and get all finalized language posted at the hyperlink provided. Drummond will validate that mandatory disclosure statements are conspicuously posted, include sufficient detail and utilize plain language. Drummond will also validate that all required product information is also posted at the hyperlink.

Reactive Surveillance

Reactive Surveillance refers to surveillance activities initiated by entities other than Drummond Group. These are principally from 1.) complaints or other related information received from any entity regarding certified Health IT technology and 2.) returning inherited certification requests.

Certified Health IT Complaints

Complaints on certified Health IT systems can be received through numerous ways, including at ehrcomplaints@drummondgroup.com.

The first step is investigating the complaint to determine if it has merit regarding functionality of certified criteria. As complaints are received on certified Health IT products, Drummond Group contacts the complaining party with additional questions to determine if the issue indicated in the complaint is within scope for the certification.

If the complaint has merit to warrant further evaluation, and if the initiator of the complaint agrees, Drummond Group will connect the initiator (typically a user of the Health IT system) and the developer of Health IT system, and Drummond Group will allow both parties to work on resolving the issue while Drummond Group monitors the situation. Drummond Group will also conduct a complete and through investigation of the issue by interviewing all personnel and examining all data relevant to the complaint. If the issue is determined to be a non-conformity, then Drummond Group follows the process for corrective action procedures as described in this plan. Per Drummond's normal process for handling complaints, a complaint is not considered closed until it is verified that the user is satisfied with the resolution or no response is received from the user within a reasonable timeframe. The summary of all complaints and resulting investigations are documented on The CHPL and reported to ONC through the Quarterly Surveillance Report.

In addition, if this issue was previously reported to the developer, Drummond Group will evaluate the vendor's previously submitted Complaint Process Summary from its Complaint Certification Information Review document. Also, the Drummond Group MSA for certification requires the developer to keep a log for all complaints received and for Drummond Group to have access to this log upon request. Drummond Group will determine how the vendor responded to this complaint. If developer did not adequately address this complaint based on their submitted processed, developer may be subject to further surveillance activities.

Inherited Certified Status Requests

Per the ONC guidance, Drummond Group policy currently dictates that after every third attestation (request for inherited certification) of certified Health IT, the product is flagged for retesting in a controlled test environment. Criteria are selected for retesting, taking into account the ONC prioritized criteria and other criteria certified by the Health IT product. Only upon successful retesting of all selected criteria can the EHR product be recertified. Any failures, including those resolved by the vendor in the course of testing, are reported to the Drummond Group Review/Decision Maker for consideration in recertification.

Additionally, developers return an Attestation of Adaptations and Updates each quarter which specifically calls attention to safety related capabilities. When a developer that has certified its Health IT technology with Drummond Group returns and submits an attestation of changes/updates to their product, Drummond Group reserves the right to test their product to ensure that what they have changed has not affected the certification criteria.

Identifiable Result

An Identifiable result is a surveillance activity conducted by Drummond Group that does not result in a non-conformity. The most common example of this is a bug or issue in certified technology that is discovered and fixed by the developer rather than identified by Drummond Group reactive surveillance. The change made by the developer may be tested at the of discretion of Drummond Group to confirm that the feature complies with the certification criterion. A Surveillance activity will be added to the CHPL at the end of the quarter in which it was identified and will be summarized on the ONC Quarterly Report.

In-The-Field Testing

The in-the-field testing may cover the ONC's prioritized criteria when applicable will and follow the guidance of the In-the-Field testing section of this document. If the selected Health IT Module is not certified to one of the prioritized criteria, that function will simply not be tested.

In addition to actual testing, Drummond Group may also engage providers on the disclosure statements of the developer to confirm the veracity and the developer's adherence to their complaint process will be assessed.

Random Surveillance

Random surveillance will be conducted on the usability of a developer's API as well as other certification criteria.

API surveillance

Drummond will conduct annually a random sample of at least 8 developer's API's using the Interoperability Hub. Drummond will report findings to both the developer and the ONC. In the event a non-conformity is found, Drummond will follow the corrective action listed below in this surveillance plan.

Certification Criteria Surveillance

Annually, Drummond will conduct random surveillance on a developer's certified product to ensure that the developer is maintaining their product to the certification criteria. In the event a non-conformity is found, Drummond will follow the corrective action listed below in this surveillance plan.

Methodology

Drummond created a randomized selection tool to identify 2% of certified products for random surveillance. Drummond may apply an appropriate weighting value to the sampling. Drummond believes it is in the best interest of the program to give different weights to EHRs that have a large user base compared to those with a smaller deployment. This is determined based on Promoting Interoperability attestation data from the HealthData.govAPI. However, while a weighted system has been applied, giving the respective products a higher weighted chance of selection, all Drummond certified products are included in the randomized selection tool and any product is eligible for random selection.

Real World Testing

Developers are required to submit their Real-World Testing Plans to their ONC ACB annually, beginning in 2022. Drummond will review and approve each test plan and post it to the CHPL by December 15th of each year. Developers are required to submit Real World Testing Results to their ONC-ACB annually, beginning in 2022. Drummond will review and approve test results and post it to the CHPL by March 15th of each year. In the event a test plan is not received and approved by Drummond, and results are not received by March 15th of each year, a Corrective Action Plan will be issued by the ONC ACB and if the plan is not submitted the developer is subject to ONC Direct Review.

Developers are required to notify their ONC-ACB within 30 days of finding a non-conformity during their Real-World Testing, Drummond will evaluate each identified non-conformity to determine what additional surveillance actions are needed. Furthermore, failure to report an identified Real World Testing non-conformity within the 30-day required timeframe constitutes a non-conformity to the Conditions of Maintenance and Certification and a Corrective Action Plan may be issued for failure to submit in the timeframe and/or the non-conformity to certified criterion.

Bi-Annual Attestations Condition and Maintenance of Certification

Developers are required under the Condition of Certification to provide an attestation, as applicable, to compliance with the Conditions and Maintenance of Certification. Developers must submit their attestation every 6 months starting on April 1, 2022. The attestation window is open for 30 days, if the developer makes no submission, they will be issued a Corrective Action Plan, the developer will have 30 days to remediate, if no remediation is obtained the developer will be referred to the ONC for Direct Review.

Please refer to the Attestations CCG for Attestations Timeline, future submission cycles, and the Conditions of Maintenance of Certification requirements.

Reporting Results

Per the ONC guidance in the 2015 Edition Final Rule, surveillance activity will be reported on a regular basis. Refer to the section of this plan on surveillance submission for more information.

Overview of Disclosures

Per the ONC requirements of certification, developers must fully disclose several aspects of information regarding their certified Health IT product.

Developers must conspicuously post the following information on their website:

- Certified Product Information
  - Developer organization name
  - Date the product was certified
  - Product name and version
  - Unique certification number
  - Certification criteria to which the product has been certified
  - CQMs to which the product has been certified
  - Any additional software the certified product relied upon to demonstrate its compliance with certification criteria
  - ONC Disclaimer: “This Health IT Module is 2015 Edition compliant and has been certified by an ONC- ACB in accordance with the applicable certification criteria adopted by the Secretary of Health and Human Services. This certification does not represent an endorsement by the U.S. Department of Health and Human Services.”

- Costs. Drummond looks for the following components when assessing disclosures of additional costs:

- The purpose of the Mandatory Disclosure is to inform. Therefore, it must include a description of the capability and costs in plain language. Plain language means a description that is no more technical than how it would be explained in marketing materials.
- The requisite plain language also applies to the title of this information on the website and in marketing materials/communications.
- This information should be easily accessible and clearly visible in a logical location on the website. While this information is not required to be on the homepage, it should be no more than a few clicks away and placed on a page to which a provider would logically navigate for this type of product information.

- The costs, and fees are regarding anything within the scope of the certified functionality, not only costs in meeting the Promoting Interoperability measures.
- If there are no costs related to a particular certified capability, that information must be clearly and explicitly stated.

At the time of certification, developers are given their language seal and logo mark in the form of a Drummond Group-issued notification of certification with instructions for its display and use. The developer's mandatory disclosure language is also collected prior to certification.

Mandatory Disclosure and API Documentation Surveillance

Once a certified technology or Health IT Module is certified, developers are typically allowed a grace period to update their website and subsequent marketing information with correct certification mark and disclosures.

Monthly, the Drummond Group Surveillance Program Manager reviews some of the Health IT products certified by Drummond Group Certification Body to confirm that the following are properly displayed:

- ONC Certified Health IT Certification and Design Mark ("ONC Health IT Mark") *
- ONC disclaimer and certification information
- Mandatory Disclosure of Costs
- API Documentation that includes the Terms of Use

**Note: Developers are not required to use the ONC Health IT Mark in their advertising, but if they do, surveillance of the Mark's use is conducted in the same manner as other web surveillance activities. For a given 12 months, the Surveillance Administrator or assigned team member reviews each website of the developer to ensure proper use of the Mark.*

Upon review, the products are classified as "Compliant" or "Non-Compliant", and developer contacts are notified via email for compliant and non-compliant status. For non-conformities, developers are notified of the issue and given 10 business days to comply. Follow up by phone is conducted if no response is received, and the Certification Body is notified after 5 additional days of non-response. Compliant products are re-reviewed upon certification of newer versions, as well as when time permits.

Non-conformities

In Mandatory Disclosure Reviews and information submitted as complaints or from other sources, a developer may be found non-conformant with the proper display of a certification logo, disclaimer or disclosure. Many non-conformities deal simply with minor typo corrections or errors that do not make a major impact in the application of this information to the general public. In those cases, the developer must still make the necessary corrections, but they will be treated as a "minor" non-conformance.

However, in cases where major aspects of disclosure are omitted or incorrectly stated, the issue is identified as a major non-conformity of website disclosures and will be reported as such. Details on procedures for corrective actions and submission of corrective action findings are found in later sections of this plan.

Surveillance of Mediums other than Website

The disclosure requirements apply to all aspects of all marketing materials, communications statements, and other assertions related to the Health IT Module's certification. However, it may not be realistic for the developer to include all required certification language, marks and disclosures on every medium (e.g., pamphlet or PowerPoint slide presentation at conference). In that case, it is acceptable to include a hyperlink/URL pointing directly to the website containing the required information (see ONC FAQ: https://www.healthit.gov/policy-researchers-implementers/46-question-2-14-046).

Drummond Group does not actively initiate surveillance on non-websites, such as requesting that copies of print material be sent to Drummond Group to review. However, if Drummond Group becomes aware of this material and determines it is not in compliance with the required certification language, marks and disclosures, the developer would become subject to surveillance procedures and non-conformance as discussed in this plan.

Quarterly Attestation

Health IT developers are required to provide a record of all adaptations and updates, including changes to user-facing aspects, made to certified health IT on a *quarterly basis* each calendar year.

The Certification Body will generate attestation tasks in the Drummond Customer Portal for all Drummond-certified developers/products. Developers will have at least 2 weeks from the end of the quarter to complete the attestation.

After each review of each attestation, the Certification Body will determine one of the following attestation decision options:

Option One. **No retesting or recertification is needed**. The Client is notified via the Customer Portal and the status will read “Reviewed-Completed”.

Option Two. **No retesting is needed, but new certification is needed.** The Client is notified via email and Customer Portal advising of the decision with regard to the certification. A copy of the email is uploaded to the client’s Box folder. Any necessary certification information is issued.

Option Three. Retesting is needed. The Client is notified via email and the Customer Portal with a status of “Reviewed-Task Created” of the decision. A copy of the email is uploaded to the client’s Box folder. The Client’s Test Proctor is notified. In turn, the Proctor will contact the client to schedule a test date.

In-The-Field-Surveillance

Purpose and Use of In-the-Field Surveillance

Successful testing performed in the controlled environment of a developer's system is the initial action needed to award certification. However, the ultimate purpose of certification is to assure developers, end users and patients that certified Health IT works as intended.

In order to fully evaluate certified health IT, surveillance of the certified Health IT must be conducted in a production environment. This surveillance is called "in-the-field" surveillance.

In-the-field surveillance is used primarily when investigating complaints on the certified Health IT system where further analysis is required. Thus, in-the-field surveillance is triggered any time Drummond Group requires additional information on the functional capabilities of a certified Health IT Module that cannot be determined through testing in a controlled test lab environment as an effective means to meet the goals and intentions of the ONC Health IT Certification Program.

Methodology and Approach of In-the-Field Surveillance

Doing in-the-field surveillance testing requires support from the end user to allow Drummond Group into their production environment and access to their Health IT system. In fact, support and access by the end user is implicit in administering any in-the-field surveillance.

When conducting in-the-field surveillance testing in the production environment, the surveillance test proctor will utilize several factors to arrive at the test methodology and data to be used in the setting. This includes:

- ONC criteria and, if applicable, the CMS Promoting Interoperability requirements
- End user proctor sheets derive from ONC approved test procedures
- Workflow of the provider or hospital setting
- Scenario(s) generating any reported non-conformities (if necessary).

The goal is to follow the spirit and direction of the ONC criteria being evaluated while mimicking the normal workflow of the provider. Also, Drummond Group may consult the developer to ensure the product is configured properly according to published instructions available to the provider.

For complaint-driven, reactive in-the-field surveillance, the testing will be around the reported non-conformance. As a result, the actual test procedure steps may be unique to that specific complaint. Regardless of the situation, the final in-the-field test steps and data used will be documented for any necessary reporting.

To supplement in-field-testing, other elements of surveillance can be incorporated or utilized to maximize the results. This can include consulting user surveys or feedback, developer complaint logs and test results from the controlled test lab environment.

Though support from hospitals or providers are crucial, in-the-field surveillance typically involves the developer at some stage. When doing in-the-field surveillance, it is the intent of Drummond Group to do everything possible to not make the effort adversarial or divisive between the end user and their vendor, but instead work to make it a cooperative effort. In cases where an end user has filed a complaint but wishes to remain anonymous, a similar approach is taken to maintain mutual respect across all parties while still keeping the main goal of achieving or confirming compliance to certified capabilities in the production environment.

In-the-field surveillance typically involves testing or evaluation of the Health IT Module in a production environment, but this type of surveillance can also involve evaluation of potential non-conformities based on in-the-field the surveillance of developer disclosure requirements. Issues reported using Direct Messaging and FHIR API's can be tested using the Interoperability Hub.

Through submitted complaints or other sources of information, Drummond Group may determine that a developer did not fully or accurately disclose aspects of the certified product. In-the-field surveillance can be used to ensure the required public disclosures of certification status are accurate. This can then lead to issuing a non- conformance finding (NCF) to the developer.

Any findings, analysis or conclusions from in-the-field surveillance will be documented in the quarterly surveillance updates submitted to ONC and in the individual corrective action findings submitted to the CHPL.

Protection of PHI during Complaint Audits

It would be Drummond Group's preference that only fictitious, but realistic, patient data be used to perform in-the-field testing. However, ONC has stated that as an ONC-ACB, Drummond Group may view Protected Health Information under 45 CFR 164.512(d) *Standard: Uses and disclosures for health oversight activities*. See also this ONC FAQ for more information: https://www.healthit.gov/policy-researchers-implementers/45-question-12-13-045.

If Drummond Group observes protected health information, it will be kept confidential and not shared in any public reports, such as the quarterly surveillance updates or in the individual corrective action findings submitted to the CHPL.

Corrective Action Procedure

Purpose of Corrective Action

Through surveillance, Drummond may determine if a Health IT Module does not conform to the requirements of its certification. This could occur through various means, including randomized surveillance testing or from user complaints. This is considered a non-conformity of certification and must be resolved in order to remain in good standing for certification.

A single complaint or even surveillance testing error does not automatically create a non-conformity, and Drummond Group will be diligent in confirming the issue is a true certification non-conformity rather than simply a user-driven error or other issue not impacting the compliance assurance of the certification. However, upon confirming a true non-conformity, Drummond Group must engage the developer to fully resolve the issue and regain the necessary confidence in the certification.

Process of Corrective Action Notification and Resolution

1. Non-conformity (NC) is identified and confirmed by Drummond Group through one or multiple means of surveillance.
    a. In Step 2 below, the developer of the Health IT Module is officially notified of the NC. However, in Step 1, Drummond Group may engage the developer to help determine the nature of the issue and allow the developer to provide all relevant facts and circumstances before confirming the issue at hand is a true NC.
    b. Non-conformity in the area of Mandatory disclosures and API Documentation are often the result of confusion in expectations or basic typos. For these types of occurrences, a developer may be able to quickly resolve the issue on its website after notification from Drummond Group before needing to issue a formal notice of non-conformity.
2. Drummond Group issues a Non-Conformance Finding (NCF) to vendor. The NCF includes a description of identified NC and summation of surveillance activities that led to its discovery.
    a. Before issuing a NCF, Drummond Group reviews the material to confirm information identifying the customer, user, practice, provider or health care location involved with the surveillance has been removed unless explicit approval has been obtained in order to assist the developer in resolving the issue.
3. The developer has a two-week window to dispute or comment on NCF. Drummond Group takes into consideration the comments of the developer and may overturn the original NC(s), but this is the sole determination of

Drummond Group. Unless Drummond Group explicitly indicates the NC is resolved, the developer must continue the plan to address the NCF.

4. Upon receipt of the NCF, vendor generally has 30 days to return a Corrective Action Plan (CAP). Drummond Group provides a template/guideline for the CAP. While 30 days is the typical timeframe, Drummond Group reserves the right to adjust this time frame based on the nature and urgency of resolving the issue.
    a. If the CAP is not returned in the appropriate timeframe, Drummond Group will take necessary actions as required by the ONC Surveillance Guidance to suspend or terminate the health IT's certification.
5. Upon receiving the CAP, it is reviewed to confirm
    a. Description of identified NCs
    b. Assessment of how widespread or isolated the NC(s) are within their customer base
    c. How the developer assessed the scope and impact of the NC, including which customers are impacted
    d. How the developer will notify all affected or potentially affected customers and users of NC(s)
    e. How the developer will ensure all potentially affected customers are notified of the problem and its plan for resolution
    f. How developer will resolve the NC(s) at all affected or potentially affected customers and users
    g. How the developer will ensure all issues are in fact resolved
    h. Timeframe of the corrective action including when all action will be completed
    i. Any other additional information relevant to the NC(s)
6. After the CAP is reviewed, Drummond Group may return it with comments and requests for alterations.
7. Once the CAP is accepted by Drummond Group, it will be signed by both Drummond Group and the developer.
8. As the developer completes actions required in the CAP, Drummond Group will remain available to discuss the NC with the developer to provide appropriate support as a certification body.
    a. In the process of resolving the NC, the developer may determine additional time is needed to fully resolve the issue. In that situation, the developer must request an amendment to the CAP and that amendment must be approved by Drummond Group. Based on this information, Drummond Group may elect to adjust the CAP scope or timeline.
9. Once the NCs are resolved according to the CAP, the developer notifies Drummond Group. The developer submits a Corrective Action Plan

Attestation (CAPA) that indicates all actions for NC resolution have been accomplished according to the CAP.

10. Drummond Group may conduct re-testing of the certified capability with the developer as well as in-the-field review to validate the fix.
11. If NCs are not resolved and completed in the agreed upon timeframe, Drummond Group will take necessary actions as required by the ONC Surveillance Guidance to adjust, suspend or terminate the health IT's certification.

Submission of Corrective Action Findings

Drummond Group will update ONC via the CHPL of surveillance results and status at the following stages of surveillance:

- Issuance of Non-Conformance Finding (NCF)
- Upon the signing of the Corrective Action Plan (CAP)
- Upon successfully resolving the NCs identified in a CAP

These updates will be associated with the respective CHPL product number to identify the certified product. All information required by the ACB Principles of Proper Conduct shall be included.

Also, Drummond Group will submit on a rolling basis the status of both reactive and proactive surveillance, including those with a CAP, to ONC Jira Ticket opened by the ONC for the following periods:

- January 1 through March 31 – Due April 15, 2022
- April 1 through June 30 – Due July 15, 2022
- July 1 through Sept. 30 – Due October 15, 2022
- Oct. 1 through Dec. 31 – Due January 15, 2023

Beyond the information normally collected in the randomized surveillance and CAPs, Drummond Group will provide analysis on the degree with which the developers in this surveillance report followed their own stated complaint processes as collected by Drummond Group on issuing certification. If a developer is found to have not followed its process, the developer must make a correction to their plan or their internal complaint handling process to ensure they align.

Before any surveillance information is submitted to ONC, it will be reviewed to ensure no sensitive information is included, such as identity of providers, locations or practice sites involved with surveillance.

Prioritized Certification Criteria

According to ONC Surveillance Guidance provided in the Program Policy Resource #18–03; https://www.healthit.gov/sites/default/files/page/2018-10/SurveillanceResource_1.pdf, the following criteria have been identified as prioritized elements of surveillance:

- Interoperability and Information Exchange
  - 45 CFR § 170.315(b)(1) Transitions of care – receive, display and incorporate transition of care/referral summaries
  - 45 CFR § 170.315(b)(6) Data Export
  - 45 CFR § 170.315(e)(1) View, download, and transmit to 3rd party
  - 45 CFR § 170.315(g)(6) Consolidated CDA creation performance
  - 45 CFR § 170.315(g)(7) Application Access – patient selection
  - 45 CFR § 170.315(g)(8) Application Access – data category request
  - 45 CFR § 170.315(g)(9) Application Access – all data request
  - 45 CFR § 170.315(h)(1) Optional -Transport methods and other protocols - direct
  - 45 CFR § 170.315(h)(2) Optional – Transport methods and other protocols – Direct, Edge Protocol, and XDR/XDM
- Safety-related
  - 45 CFR § 170.315(a)(4) Drug-drug, drug-allergy interaction checks for CPOE
  - 45 CFR § 170.315(a)(9) Clinical decision support - CDS
  - 45 CFR § 170.315(b)(2) Clinical information reconciliation and incorporation
- Security
  - 45 CFR § 170.315(d)(2) Auditable Events and Tamper-Resistance
  - 45 CFR § 170.315(d)(7) End-User Device Encryption
- Population Management
  - 45 CFR § 170.315(c)(1) Clinical quality measures – record and export