Gaming Laboratories International, LLC dba SLI Compliance

ONC-ACB 2020 Surveillance Plan

Revision: 1.1

Document ID: ACB-Surv-Plan-20

Issued: January 20, 2020

4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

Document History

Rev.	Date	Change
1.0	September 24, 2019	Initial Version
1.1	January 20, 2020	Updated references to ONC Program Policy Guidance documents, added 2015 prioritized criteria to Appendix A, clarified 2.2.5 re customer lists

Contents

1 Introduction

This Plan describes the annual surveillance approach that SLI Compliance (SLI) will follow, as an Authorized Certification Body, for 2020. SLI is committed to conducting surveillance in an impartial and transparent manner; complying with the requirements of relevant federal regulations (specified in 45 CFR Part 170); and adhering to the requirements of ISO 17065:2012. SLI's surveillance approach is directed by the program requirements and guidance of the Office of the National Coordinator for Health Information Technology (ONC).

To submit information to SLI about any SLI Certified product, please email us at ACB@slicompliance.com, or go to http://www.slicompliance.com/services/testing-certification-health/sli-acb-certified-products-feedback-and-complaints/. The web link allows for anonymous or non-anonymous reporting of information/complaints. SLI will follow up on information received and will further investigate credible information regarding any SLI Certified product's conformity to the relevant requirements.

Developers of ONC certified Health IT are required to adhere to program requirements to maintain certification. One key element is cooperation with the ACB to support ONC program activities, including but not limited to inquiries relevant to the certified criteria and requirements; surveillance; requests for customer lists, complaint logs and updates; and corrective actions. Likewise, SLI's approach is to treat developers fairly, conduct activities in a transparent manner and respond to developers' inquiries.

1.1 References

This document incorporates by reference the following ONC guidance documents, released in October 2018:

- ONC HEALTH IT CERTIFICATION PROGRAM Program Policy Resource #18–03: Surveillance Resource (10/5/2018)
- ONC HEALTH IT CERTIFICATION PROGRAM Program Policy Resource #18–01: Post-certification Assessment of Program Requirements (10/5/2018)
- ONC HEALTH IT CERTIFICATION PROGRAM Program Policy Resource #18–02: Disclosure of Material Information (10/5/2018)

This document also references the current version of SLI's Certification Program Manual, available on http://www.slicompliance.com/services/testing-certification-health.

2 Surveillance Approach

SLI conducts both proactive and reactive surveillance based on the requirements of ISO 17065 as well as ONC guidance.

Proactive surveillance includes two main areas. First, SLI may execute surveillance of a random sample of SLI certified health IT products each year, based on the ONC's stated guidelines and priorities. Second, SLI will conduct regular routine surveillance to review the use of ONC and SLI certification marks, developer disclosures, and requirements around websites and communications.

SLI conducts reactive surveillance to follow up on complaints regarding certified products. SLI will also perform surveillance in response to three or more requests for inherited certifications for a given health IT product.

Prior to initiating surveillance, SLI will consult the relevant regulations and resources, including 45 CFR 170.556 (https://www.ecfr.gov/cgi-bin/text-idx?SID=429be73364bbb51d21cd984f70c60a0f&mc=true&node=se45.1.170_1556&rgn=div8), any other relevant criteria in 45 CFR section 170, and the current ONC guidance (https://www.healthit.gov/topic/certification-ehrs/onc-health-it-certification-program-guidance).

2.1 In-the-field Surveillance

One condition of product certification in the ONC Health IT Certification Program (ONC program) is ongoing surveillance. Some of these surveillance activities take place at the location where the technology is employed by end users. SLI will use in-the-field testing and observation as needed for surveillance activities. For complaints, SLI will first gather and examine evidence collected by other means and determine whether more information is needed to determine conformity, requiring in-the-field surveillance. For example, a reported problem may not occur in a controlled environment but is reported in the field, or a problem may occur intermittently but not in every instance. A high level of complexity surrounding a problem may also necessitate in-the-field surveillance.

2.1.1 Planning and Conducting In-the-field Surveillance

When planning surveillance in the field, SLI will first identify the certification requirements to review. (Specific approaches to proactive surveillance and complaint investigations are detailed below.) In addition, SLI will consider the context of the product's marketing, implementation and use. This includes the developer's targeted users, situations of use and real-world use cases.

The first choice for selecting a location is to use the location where the reported problem occurred. If this is not possible, such as for an anonymous complaint, SLI will attempt to identify a similar implementation.

Also, the first option in many cases is to conduct the testing, observation or other investigation remotely; on-site testing will be conducted if SLI determines a need for additional information that can't be obtained remotely.

SLI's in-the-field activities may include tests based on the test scripts, methods and recording techniques used by SLI's ONC-ATL. SLI is required by the ONC to determine whether the use of test data would yield similar product behavior and be equally comprehensive to data used in production systems. This analysis is based on the issue identified, its complexity, and the options for use of the relevant product feature(s).

SLI recognizes that some capabilities are within the scope of the certification criteria but cannot be fully tested in a controlled environment. For reactive surveillance, SLI will identify such capabilities (relevant to the known problem or complaint) and will plan other types of observations to evaluate conformity to the requirements in production environments. It may be necessary to consult with the developer and/or end users to determine the best approaches within the workflow at the production site.

In-the-field surveillance requires that SLI engage and work with developers and end-users to analyze and determine the causes of issues. From the developer viewpoint, open communication with the ACB in specified areas is an important part of the service agreement for continuing certification and contributes to the integrity of the ONC certification program. Developers of certified products are required by the program to provide certain information back to the ACB, including complaints relevant to the certification criteria, disclosures and product changes. This also includes responses to requests for information or surveillance that fall within the program's specifications.

In preparation for in-the-field observation and testing, SLI will contact the developer and end user to communicate what issues or requirements are slated for observation, the timeframe, and other details. SLI will allow sufficient time for the location to prepare and to allocate resource time and will also work with the provider to minimize the burden of participating. When both the end user and the developer are involved, SLI aims to encourage and facilitate a respectful, collaborative process. When a complainant is an end user who wants to remain anonymous, SLI will respect confidentiality in the investigation of the complaint.

When a health care provider does not cooperate with SLI's surveillance activities or frustrates those activities, SLI will carefully and accurately document its efforts to complete in-the-field surveillance for that product and location, including a provider's failure to

cooperate in good faith. SLI will provide this information in its periodic surveillance reports to the ONC.

SLI will observe and evaluate the certified capabilities, including consistency and reliability of performance, and will record detailed notes. If potential non-conformities are observed, SLI will investigate the cause(s) to determine whether and to what extent they are under the control of the developer.

In addition to in-the-field observations, SLI will also gather additional information. Some example sources that SLI may use are:

- Developers' websites, marketing materials, and other communications
- Complaint processes, logs and records of resolution
- Review of previous test records and developer attestations
- User surveys or other feedback
- Observation and analysis of the product in a controlled environment
- Contract between the developer and user(s)
- Evaluation of the product at additional sites
- Other relevant information provided by the developer

Survey program: SLI may develop end user surveys to gather information regarding the certification criteria and other certification requirements. SLI analyzes the criteria to be investigated and develops a series of questions that ask users in plain language about their experience using the product in the areas being evaluated. (Example: Regarding [Software name, version], does your electronic records software's audit log of user activity allow you to sort the audit log report according to each data element?). These surveys may be sent to a randomly selected set of user contacts from the most recent customer list supplied by the developer, or they may be sent to a selected set of users with a specific implementation to investigate a reported problem. After a reasonable time (about a week if the surveys are emailed), SLI will remind the recipients who did not respond to the surveys. SLI will follow up on any issues identified in the survey responses. Follow-up may include asking the respondent for additional details, expanding the survey pool, and/or initiating other surveillance activities as appropriate.

2.1.2 Observation Records and Nonconformities

SLI will retain records of all relevant observations and test outcomes, which will include all identified nonconformities. These records will also include relevant details and their sources where appropriate, SLI's activities and analysis, and dates. SLI personnel conducting

reactive surveillance are encouraged to keep a log of activities, references, persons contacted, analysis and follow-up, and dates, in order to establish a timeline of events.

NOTE: During surveillance, SLI may observe protected health information (PHI). This information will be kept strictly confidential and not included in reports such as the regular surveillance reports to the ONC or in the corrective action notifications submitted to the CHPL. SLI endeavors not to retain any PHI and shall adhere to its internal procedures to protect any sensitive information if it must be recorded.

If any nonconformities are discovered, SLI will work with the developer (and the resources at the implementation site as appropriate) to identify the root cause. The Corrective Action section details this process.

In addition to nonconformities related to technical capabilities, another type of issue may result from business or implementation practices of the health IT developer that negatively affect functioning of the certified product in the field. Such an issue, when substantiated, is considered to be a nonconformity against certification requirements. Another category of nonconformity is the non-disclosure of material information about limitations or attestation provided with regard to additional types of costs associated with a certified health IT product. For more information, see the SLI Certification Program Manual section "Suspension, Withdrawal, or Revocation of Certification".

2.2 Proactive Surveillance

As part of SLI's certification program and depending on current ONC guidance, SLI may conduct random surveillance of a percentage of certified products for which SLI is responsible (above and beyond routine surveillance as described below). The selection method is described below under Random Surveillance. For each selected product, SLI shall perform surveillance of each capability (where applicable) prioritized by the ONC.

SLI will assess:

- Health IT's conformity to the prioritized certification criteria described in the ONC's "Prioritized Elements of Surveillance," plus any other criteria to which the product is certified, at SLI's discretion.
- The adequacy of developers' user complaint processes.
- Developers' compliance with the mandatory disclosure requirements of 45 CFR § 170.523(k)(1).*
- Appropriate use of the ONC and SLI Certification Marks.*

2.2.1 Routine Surveillance

Each quarter, SLI requires developers to provide a list of all complaints relevant to each product's certification. SLI reviews these logs for information regarding compliance with the certification criteria and requirements. SLI will follow up on complaints and resolutions, which may include requesting additional information from the developer and/or initiating reactive surveillance. For instance, SLI will gather more information and may initiate surveillance if there is a suspected non-conformity that has not been fully resolved (or the resolution is not adequately described) or when the problem may have additional impacts beyond the ones the developer has addressed.

In addition, SLI conducts routine proactive surveillance on each actively certified product annually, within each 12-month period after certification, covering the areas marked with "*" above. This routine surveillance involves monitoring websites related to the certified health IT (which will always include the Mandatory Disclosures URL linked from the CHPL for the product, plus other developer web pages describing the product) and may also include review of other publicly available materials. Additionally, for follow-up purposes or based on SLI's experience with a particular product, SLI may request information from the product developer regarding certified products.

2.2.2 Random Surveillance

The ONC announced it will exercise its discretion not to enforce the random surveillance requirements that are detailed in 45 CFR 170.556(c)(2) (https://www.healthit.gov/sites/default/files/ONC_Enforcement_Discretion_Randomized_Surveillance_8-30-17.pdf). If this guidance changes, or as needed to maintain the integrity of the SLI Health IT Certification Program, SLI may conduct random surveillance. In such case, SLI shall select from the products to which SLI's ONC-ACB has issued a certification (i.e., all active certifications). SLI will implement weighting techniques that account for the number of implementations of certified products and risks identified during the testing process. These risks include the risk that a product may fail to meet certification requirements in the field due to difficulty of completing the testing or lack of readiness (e.g., multiple re-tests needed).

SLI shall exclude from this surveillance any product for which non-routine proactive surveillance was conducted within the last 12 months.

Prior to randomly selecting products for proactive surveillance, SLI will assign weights to certified products based on how many users have adopted the certified products and how many retests were needed during the testing phase. This increases the probability that the certified products selected for surveillance will include products with larger numbers of users and/or higher risks of failure to meet the test criteria in the field. SLI will check the

customer lists provided by the developers of SLI Certified products to determine the number of providers using each vendor's certified product(s). Based on the numbers of implementations, SLI will enter products and their weights into a random number generator to determine the products selected.

For each selected product, SLI will again use the random number generator to randomly choose sites where the product is in use. SLI will inform the developer of the surveillance and will contact the selected sites. SLI will attempt to gather information from those sites using emailed surveys and/or calls. Any issues identified in the surveys will be followed up with further information gathering. (More details on surveys follow below.)

2.2.3 Prioritized Capabilities and Other Prioritized Elements

When SLI selects a product for randomized surveillance, the evaluation of the product in the field shall include the assessment of any capabilities that are (1) within the scope of the certification criteria to which the technology is certified and (2) associated with any certification criterion prioritized by the ONC. 45 CFR §170.556(c)(1). SLI shall include all applicable elements from the prioritized capabilities listed in the ONC's guidance released in 2018. Any other certified areas may be assessed at the discretion of the SLI assessor.

Prioritized criteria are listed in Appendix A.

SLI shall address each of the additional ONC prioritized elements. These include assessments of developers' disclosures, assessment of potential nonconformities related to implementation or business practices, adequacy of developers' user complaint processes, and appropriate use of the ONC Certification Mark.

Surveillance of prioritized capabilities and elements may include further assessment by SLI's ACB or additional evaluation by an ONC-ATL. As needed, SLI may request additional information, such as sample data outputs and live demonstrations of the product in the field. SLI may request additional information from the developer, including documentation to substantiate that previously certified functionality has not been compromised.

2.2.4 Exclusion and Exhaustion

When a certified product has been selected for randomized surveillance, SLI shall make a good faith effort to conduct remote information gathering for the selected product at the first set of randomly-selected locations (typically 5). If, after making this good faith effort, SLI cannot complete the surveillance at the selected locations for reasons beyond our control, SLI may exclude such locations and substitute another set of locations (also typically 5) that meet the random selection requirements described above. Similarly, if SLI exhausts all available locations for a particular certified product, we may exclude that product.

In the case of exhaustion or of 2 unsuccessful attempts at getting information from the randomly selected users, the excluded certified product will be counted towards the minimum number of products SLI is required to surveil during the calendar year surveillance period (if applicable). SLI shall document our efforts to complete surveillance for each product and at each location. Any information regarding the selection and exhaustion of locations will be reported in regular surveillance reports to the ONC.

2.2.5 Developer Customer Lists

SLI may obtain and integrate health IT developers' customer lists into its randomized sampling and other aspects of proactive and reactive surveillance. SLI reserves the right to request customer lists as needed. Additionally, before initiating any in-the-field surveillance activities, SLI will obtain a customer list from the selected health IT developer.

Access to accurate customer and user lists is essential to an ONC-ACB's ability to contact users for in-the-field surveillance and to conduct surveys and other activities necessary to obtain and synthesize information about the performance of certified health IT. Therefore, if a health IT developer refuses to provide this information to SLI, SLI may regard the refusal as a refusal to participate in surveillance under the ONC Health IT Certification Program and institute appropriate procedures, consistent with SLI's accreditation to ISO 17065, to suspend or terminate the health IT certification per 80 FR 62601, 62716.

2.3 Reactive Surveillance

SLI will initiate surveillance of a certified product whenever it becomes aware of information that would cause a reasonable person to question the health IT's continued conformity to the requirements of its certification. Reactive surveillance occurs mainly in response to complaints from end user customers or any other entities regarding certified health IT product(s), and also where there are repeated inheritance requests (products with 3 or more inherited certified status requests). Reactive surveillance may include in-the-field surveillance as needed.

When SLI becomes aware of a complaint that may be related to the certification criteria or other certification requirements applicable to a health IT product, SLI will investigate the complaint to determine whether the complaint is credible and substantive and the matter is in scope for the product's certification. Where a complaint appears to be in scope and credible, SLI will initiate surveillance.

SLI will obtain and analyze information of various types depending on the nature of the complaint. This information includes but is not limited to the following:

- Complaints and other information about certified health IT submitted directly to SLI or to the ONC by customers or users of certified health IT, by the ONC, or by another entity.
- Health IT developers' complaint logs, service tickets, and documentation concerning the analysis and resolution of complaints or issues reported to the developer.
- Developers' public and private disclosures regarding certified health IT capabilities.
- Information from publicly available sources (e.g., a developer's website or user forums).
- Repeated inherited certified status requests (3 or more for a single product).
- Other relevant facts and circumstances of which SLI is aware – in particular, information relevant to areas prioritized by the ONC as listed in Appendix A.

SLI will conduct a thorough investigation of the issue. This will include examining all data relevant to the complaint and may also include interviewing developer personnel. SLI shall always review health IT developers' disclosures when performing reactive surveillance and will also examine developers' complaint logs and responses to complaints relevant to the issue. To establish whether the product remains conformant, SLI will consider all information obtained including factors contributing to the issue and the scope of the impact, as well as the response from the developer and any other data collected. In-the-field surveillance will be employed if SLI determines that this approach is the best way to gather the needed information for one or more criteria/requirements, or if other methods to gather data prove insufficient.

Even where a product is shown to have the required capabilities, in some cases the developer may interfere with the user's ability to exercise these capabilities or may impose undisclosed limitations. SLI will investigate such claims, including the contract between the developer and user, the developer's communications and disclosures, and any limitations imposed by the developer that may hinder use, potentially causing a nonconformity with certification requirements.

All reactive surveillance will be documented in regular surveillance reports provided to the ONC. Details are retained in SLI's records. If SLI determines any issue to be a non-conformity, the corrective action process as described in this plan will be followed.

3 Transparency and Disclosure Requirements

As part of proactive and reactive surveillance, SLI will obtain information to ensure developer compliance with mandatory disclosure requirements. Routine surveillance is carried out by monitoring developer websites and may include reviews of other publicly

available materials. SLI reviews each developer's website and assesses whether the information shown meets ONC requirements and corresponds to the information in the developer's attestation made for product certification.

SLI may begin reviewing websites for certified products any time after certification is posted on the ONC CHPL and will typically wait at least one month to allow for developer updates. SLI performs web surveillance on an ongoing basis and will check each actively certified developer's website at least once per year. The following items will be monitored:

- ONC Certified Mark (if used – use is not required but if the mark is used, the usage must conform to ONC requirements)
- SLI Certified Mark (if used – use is not required but if the mark is used, the usage must conform to SLI Compliance requirements)
- ONC disclaimer and certification information
- Disclosure of costs and limitations in a clear and accessible manner

SLI also evaluates disclosures as part of all reactive surveillance. SLI will ask developers for their marketing materials, communications and statements, and other assertions related to the product so SLI can review these for compliance. When SLI identifies instances in which failures to disclose limitations or additional types of costs have substantially impaired their use (or could), SLI will follow up with the developer and, where appropriate, will initiate surveillance or a corrective action.

SLI will communicate any apparent issues with the above information to the developer per our Corrective Action Procedure. SLI will provide the developer an opportunity to correct any nonconformities. Please see the SLI Certification Program Manual section "Suspension, Withdrawal, or Revocation of Certification" for more information.

3.1 Surveillance of Developers' Disclosures

The developer of a certified health IT product is required to disclose (or link to a disclosure) in plain language—on its website and in all marketing materials, communications statements, and other assertions related to its certified health IT—a detailed description of all known material information concerning limitations and additional types of costs that a person may encounter or incur to implement or use certified health IT capabilities, whether to meet meaningful use objectives and measures or to achieve any other use within the scope of the health IT's certification. Such information is required if the failure to disclose it could substantially interfere with the ability of a user or prospective user to implement or use certified health IT for any use within the scope of the product's certification. Certain

kinds of limitations and additional types of costs, if known, must be disclosed. These include but are not limited to:

- Additional types of costs or fees (whether fixed, recurring, transaction-based, or otherwise) imposed by a developer (or any third-party from whom the developer purchases, licenses, or obtains any technology, products, or services in connection with its certified health IT) to purchase, license, implement, maintain, upgrade, use, or otherwise enable and support the use of capabilities to which health IT is certified; or in connection with any data generated in the course of using any capability to which health IT is certified.

- Limitations, whether by contract or otherwise, on the use of any capability to which technology is certified for any purpose within the scope of the technology's certification; or in connection with any data generated in the course of using any capability to which health IT is certified.

- Limitations, including but not limited to technical or practical limitations of technology or its capabilities, that could prevent or impair the successful implementation, configuration, customization, maintenance, support, or use of any capabilities to which technology is certified; or that could prevent or limit the use, exchange, or portability of any data generated in the course of using any capability to which technology is certified.

ONC Notes: Developers are not required to disclose information of which they are not and could not reasonably be aware, nor to account for every conceivable type of cost or implementation hurdle that a customer may encounter. “Developers are required, however, to describe **with particularity** the nature, magnitude, and extent of the limitations or types of costs.” 80 FR 62601, 62722 (emphasis in original). A developer’s disclosure must contain sufficient information and detail from which a reasonable person under the circumstances would, without special effort, be able to reasonably identify the specific limitations he or she may encounter and reasonably understand the potential costs that may be incurred when implementing and using capabilities for any purpose within the scope of the health IT's certification.

3.2 Attestation

SLI includes the transparency attestation detailed in Appendix B as part of new certification applications and in the update process for previously certified products.

In addition to ensuring that the developer has made the proper attestation, SLI shall include the developer’s attestations in the information submitted to the ONC for inclusion in the CHPL.

4 Corrective Action Procedures

The ONC has clarified that a corrective action plan (CAP) is required any time an ACB finds that a product or a developer is non-compliant with any certification criterion or any other requirement of certification, including the transparency and disclosure requirements.

When SLI determines that a certified health IT product or developer does not conform to the requirements of the relevant certification, SLI shall notify the developer of these findings and require the developer to submit a proposed CAP for the applicable certification criterion/criteria or other certification requirement. This CAP must include:

- A description of the identified non-conformities or deficiencies;
- An assessment of how widespread or isolated the identified non-conformities or deficiencies may be across all of the developer's customers and users of the certified product;
- How the developer will address the identified non-conformities or deficiencies, both at the locations under which surveillance occurred and for all other potentially affected customers and users;
- How the developer will ensure that all affected and potentially affected customers and users are alerted to the identified non-conformities or deficiencies, including a detailed description of how the developer will assess the scope and impact of the problem, including identifying all potentially affected customers; how the developer will promptly ensure that all potentially affected customers are notified of the problem and plan for resolution; how and when the developer will resolve issues for individual affected customers; and how the developer will ensure that all issues are in fact resolved.
- The timeframe under which corrective action will be completed.
- Any additional elements specified by the ONC or that the ONC-ACB deems appropriate, consistent with its accreditation. (These are based on the specific finding and guidance will be provided if this requirement is applicable.)
- A requirement that the developer attest to having completed all elements of the corrective action plan.

SLI will notify a developer when one or more deficiencies are found, along with providing a template and a timeframe for providing a CAP to SLI. The timeframe is typically 30 days, but

SLI reserves the right to adjust this timeframe based on the type of issue and the urgency of resolving it.

If the CAP is not returned in the appropriate timeframe, SLI will take necessary actions as required by the ONC Surveillance Guidance to suspend or terminate the health IT's certification.

SLI will submit corrective action information to ONC for inclusion on the Certified Health IT Product List (CHPL). This information will be updated weekly whenever the status changes.

SLI shall verify that developers have completed all requirements of corrective action specified in the approved corrective action plan. SLI requires developers to attest that the developer has completed all required elements of the plan, and then SLI validates that attestation. SLI will also verify that developers have notified all affected and potentially affected customers and users and will notify the developer of the outcome of the CAP process.

5 Submission of Corrective Action and Surveillance Information

SLI shall submit information regularly to the ONC, as described below.

5.1 Submission of Corrective Action Information

SLI will document and, at least once weekly, submit corrective action information to ONC for inclusion in the CHPL. This report will include each product that failed to conform to its certification and for which corrective action was instituted under 45 CFR § 170.556. SLI will use the CHPL product number to identify the certified products.

For each finding of nonconformity, SLI will report the specific certification requirements to which the product failed to conform. SLI is also required by the ONC to report other information about the nature, details and status of each nonconformity. Details are included in SLI's internal procedure for reporting, which includes all bulleted items from the ONC Guidance document (Program Policy Guidance #18-03, section Submission and Reporting of Surveillance and Corrective Action Information).

5.2 Submission of Surveillance Information

5.2.1 Surveillance Narratives and Corroborating Documentation

SLI shall report surveillance results to the ONC on a quarterly and annual basis. When submitting annual surveillance results, SLI will identify each instance of surveillance

performed during the calendar year and the results of that surveillance. In each case, SLI will submit a detailed narrative and corroborating documentation and evidence to support its determination, including:

- Each certified health IT product, certification criterion, and certification program requirement that was subjected to surveillance during the calendar year. SLI will use the CHPL product number to identify the certified products.
- The type of surveillance initiated in each case.
- The grounds for initiating surveillance and for deciding whether or not to evaluate the certified health IT in the field.
- Whether or not SLI confirmed a non-conformity.
- The substantial factors that, in SLI's assessment, caused or contributed to the apparent non-conformity (e.g., implementation problem, user error, limitations on the use of capabilities in the field, a failure to disclose known material information, etc.).
- The steps SLI took to obtain and analyze evidence and to arrive at its conclusions.

This surveillance plan describes in detail the process by which SLI will collect and submit all of the information described above, including the procedural aspects required by the ONC (Program Policy Guidance #18-03, section Submission and Reporting of Surveillance and Corrective Action Information).

5.2.2 Review of Developer Complaint Processes

As requested by the ACB, developers of certified Health IT products are required to provide details of their complaint handling process for complaints relating to the scope of functionality certified in the ONC program.

SLI will identify, for each health IT developer whose technology was subject to any type of (non-routine) surveillance during the applicable calendar year:

- The extent to which the developer followed its complaint process, and any observed deficiencies with its process.
- The frequency of complaints made to the developer associated with the prioritized elements in Part IV.

SLI reviews the complaint handling processes of each developer whose product is subject to surveillance to determine whether the appropriate actions were taken, along with the developer's adherence to their own complaint handling process. If any issues weren't properly addressed, SLI will follow up and will report this finding to the ONC. SLI will also

evaluate the frequency of complaints made to the developer that were associated with the ONC's areas for prioritized surveillance. Issues found will trigger SLI's Corrective Action procedure.

5.3 Due Process and Exclusion of Certain Sensitive Information

5.3.1 Meaningful Opportunity for Input and Comment on ONC-ACB Findings

SLI shall complete our review of all relevant facts and circumstances, including those raised by the developer in the course of SLI's surveillance, prior to making a non-conformity or other determination and prior to submitting its surveillance results and, where applicable, corrective action information to the ONC.

In addition, SLI shall provide a meaningful opportunity for the developer to explain any deficiencies prior to a final non-conformity determination. When the developer has provided an explanation of the deficiencies identified as the basis for SLI's determination, SLI shall include the developer's explanation (subject to any exclusions described below) in its submission of this information to the ONC.

5.3.2 Exclusion of Certain Information from Submission of Corrective Action Information and Surveillance Results

In submitting corrective action information and surveillance results to the ONC, SLI shall exclude any information that would identify any customer or user, any health care provider, location, or practice site that participated in or was subject to surveillance, or any person who submitted a complaint or other information to a health IT developer or ONC-ACB.

5.3.3 Exclusion of Certain Information from Submission of Corrective Action Information

With respect to the submission of corrective action information to the ONC for inclusion in the CHPL, SLI will not submit any information that is in fact legally privileged or protected from disclosure and that therefore should not be listed on a publicly available website. SLI may also implement other appropriate safeguards, as necessary, to protect information that, while not legally protected from disclosure, SLI believes should not be reported to a publicly available website.

The ONC requires ACBs to ensure that such safeguards are narrowly tailored and consistent with the goal of promoting the greatest possible degree of transparency with respect to certified health IT and the business practices of certified health IT developers, especially the disclosure of material information about limitations and types of costs associated with certified health IT. ONC-ACBs are required to accurately report the results of their

surveillance and to explain in detail the facts and circumstances on which their conclusions are based.

5.4 Due Date and Submission Method

Surveillance results are due to ONC quarterly in the agreed upon template. ONC will only accept electronic submissions of surveillance results (emailed as instructed by the ONC).

6 Public Accountability

SLI Compliance acknowledges that ONC-ACBs should make their annual surveillance plans publicly available after submission to ONC and that ONC may at any time publish surveillance information to the extent permitted by law.

7 Appendix A: Prioritized Criteria

2014 Edition	2015 Edition
Interoperability and Information Exchange	
--45 CFR 170.314(b)(1) Transitions of care – receive, display and incorporate transition of care/referral summaries. --45 CFR 170.314(b)(2) Transitions of care – create and transmit transition of care/referral summaries. --45 CFR 170.314(b)(7) Data portability. --45 CFR 170.314(b)(8) Optional – transitions of care. --45 CFR 170.314(e)(1) View, download, and transmit to 3rd party. --45 CFR 170.314(h)(1) Optional – Transmit - Applicability Statement for Secure Health. --45 CFR 170.314(h)(2) Optional – Transmit - Applicability Statement for Secure Health Transport and XDR/XDM for Direct Messaging.	--45 CFR 170.315(b)(1)(i) Transitions of care. --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) Transport methods and other protocols – Direct Project. --45 CFR 170.315(h)(2) Transport methods and other protocols – Direct, Edge Protocol, and XDR/XDM.
Safety-related	
--45 CFR 170.314(a)(2) Drug-drug, drug-allergy interaction checks. --45 CFR 170.314(a)(8) Clinical decision support.	--45 CFR 170.315(a)(4) Drug-drug, drug-allergy interaction checks for CPOE.

--45 CFR 170.314(a)(16) Inpatient setting only—electronic medication administration record. --45 CFR 170.314(b)(4) Clinical information reconciliation. --45 CFR 170.314(b)(9) Optional – Clinical information reconciliation and incorporation.	--45 CFR 170.315(a)(9) Clinical decision support (CDS). --45 CFR 170.315(b)(2) Clinical information reconciliation and incorporation.
Security	
--45 CFR 170.314(d)(2) Auditable Events and Tamper-Resistance. --45 CFR 170.314(d)(7) End-User Device Encryption.	--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 170.314(c)(2) Clinical quality measures – import and calculate.	--45 CFR 170.315(c)(1) Clinical quality measures – record and export.

8 Appendix B: Transparency Attestation

As a condition of certification, health IT developers must make one of the following attestations:

In the affirmative:

> In support of enhanced marketplace transparency and visibility into the costs and performance of certified health IT products and services, and the business practices of health IT developers, [Developer Name] hereby attests that it will provide in a timely manner, in plain writing, and in a manner calculated to inform, any part (including all) of the information required to be disclosed under 45 CFR § 170.523(k)(1) under the following circumstances:
>
> - To all persons who request such information.
> - To all persons who request or receive a quotation, estimate, description of services, or other assertion or information from [Developer Name] in connection with any certified health IT or any capabilities thereof.
> - To all customers prior to providing or entering into any agreement to provide any certified health IT or related product or service (including subsequent updates, add-ons, or additional products or services during the course of an on-going agreement).

- OR -

In the negative:

> [Developer Name] hereby attests that it has been asked to make the voluntary attestation described by 45 CFR § 170.523(k)(2)(i) in support of enhanced marketplace transparency and visibility into the costs and performance of certified health IT products and services, and the business practices of health IT developers. [Developer Name] hereby declines to make such attestation at this time.

-- OR –

Self-Developer:

> [Developer Name] hereby attests that it is a self-developer exempt from the disclosure requirements of 45 CFR 170.523(k)(1)(iii) and 170.523(k)(2). [Developer Name] further attests that as a self-developer it does not and will not market, sell, or license its certified Health IT Module(s).

Note that a developer's attestation under 45 CFR §170.523(k)(2) does not broaden or change the scope of the information a developer is required to disclose under 45 CFR §170.523(k)(1).

End of Document