Verification Router Service

Operational Guidance

FREQUENTLY ASKED QUESTIONS/FAQs

Version:	1
Date:	7-May -2019

Table of Contents

1. Introduction

1.1 Background

The Drug Supply Chain Security Act (DSCSA), enacted on November 27, 2013 in Title II of the Drug Quality and Security Act (DQSA), aims to help combat the threat of pharmaceutical diversion by enhancing the traceability of prescription pharmaceutical products in the U.S. The DSCSA amends the federal Food, Drug and Cosmetic Act (FDC Act)[1] to establish an interoperable electronic system for the identification and tracing of individual units of certain prescription drugs. This legislation, which preempts state and local laws, mandates that all trading partners in the supply chain be authorized and hold appropriate licenses or registrations, details requirements for verification procedures and prescribes requirements for information necessary to identify and trace the distribution of prescription products down to the smallest unit intended for sale to a dispenser. This interoperable electronic system is to be implemented in stages over the next five years across the entire pharmaceutical supply chain. By November 27, 2023, each package of applicable prescription drug product must bear a product identifier[2], which includes a unique serial number[3] that will link each saleable product unit to the selling and purchasing sources of the product in a secure, interoperable, electronic system [See § 582(g)(1)]. **One important milestone in the progress towards the 2023 deadline and full product traceability begins on November 27, 2019.** Starting on that date, each wholesale distributor is required to "verify" the product identifier on each unit (or sealed homogenous case) returned that the wholesale distributor seeks to resell.

Beginning on November 27, 2019, before a wholesale distributor may resell a returned product, "the wholesale distributor shall verify the product identifier, including the [SNI] … for each sealed homogeneous case or on each package" [§ 582(c)(4)(D)]. "Verification" or "verify" "means determining whether the product identifier affixed to, or imprinted upon on a package or homogeneous case corresponds to the [SNI] … assigned to the product by the manufacturer or the repackager…."[4] [§ 581(28)]. A manufacturer who receives a verification request from a repackager, wholesale distributor,

[1] Citations that follow to sections 581 and 582 refer to sections of the FDC Act as amended by the DSCSA and are codified at 21 U.S.C. § 360eee and § 360eee-1, respectively.

[2] The product identifier requirement went into effect on November 27, 2017, by which time manufacturers must affix or imprint a product identifier to each package and homogenous case intended to be introduced in a transaction into commerce [§ 582(b)(2)(A)]. However, on June 30, 2017, the FDA issued a Draft Guidance that provided for the agency to exercise discretion and not take enforcement action against manufacturers that serialize after November 27, 2017 but before November 27, 2018. 82 Fed. Reg. 30868 (July 3, 2017). FDA finalized the Draft Guidance on September 19, 2018. *See Product Identifier Requirements Under the Drug Supply Chain Security Act – Compliance Policy, Guidance for Industry* (September 2018), available at https://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM565272.pdf]. , Repackagers were required to affix product identifiers by November 27, 2018. [§ 582(e)(2)(A)].

[3] The product identifier is a standardized graphic in human-readable form and on a machine-readable carrier that conforms to international standards and includes the product's unique standardized numerical identifier (SNI), lot number and expiration date [§ 581(14) (definition of product identifier). The SNI is "a set of numbers or characters used to uniquely identify each package or homogenous case that is composed of the National Drug Code that corresponds to the specific product (including the particular package configuration) combined with a unique alphanumeric serial number of up to 20 characters." § 581(20).

[4] Section 581(28) also permits verification of a product identifier by "lot number and expiration date." However, once all product is serialized, there would be no reason for trading partners to verify product by lot number and expiration date when the product identifier (which includes the SNI, lot number, and expiration date (§ 581(14)) would be more accurate and efficient.

or dispenser must respond to that request within 24 hours (or such other time FDA establishes) [§ 582(b)(4)(C)]. A repackager also has 24 hours to respond [§ 582(e)(4)(C)].

This requirement will be henceforth referred to as the 2019 Saleable Returns Requirement in this document.

2. Purpose

2.1 The Pilot Study

As industry began exploring verification solutions, the Healthcare Distribution Alliance (HDA) sponsored the Traceability Pilots Work Group to focus on a pilot study of nine (9) potential methods or solutions to meet the 2019 Saleable Returns DSCSA Requirements. Through the process of evaluating nine scenarios, the Work Group acknowledged no single solution for the supply chain existed, and put forward two preferred options, keeping in mind solution cost, implementation effort, process execution, exception handling, advantages and disadvantages, and sustainability implications from both the manufacturer and wholesale distributor perspective. One of the options studied in the pilot was a Verification Router Service (or “VRS”). A proof of concept was successfully built and utilized during a live pilot, but it was only a temporary system for the purpose of the pilot. (For the full pilots report, see https://www.hda.org/resources/hda-saleable-returns-pilots-report). At the conclusion of the pilot study, the Work Group believed the Verification Router Service was the most feasible external solution due to its speed and security.

The Traceability Pilots Work Group also saw value in a verification process where a manufacturer sends to each individual wholesale distributor customer aggregated product identifier information for only the units of product that the manufacturer sold to that individual wholesale distributor; to verify a saleable return, the wholesale distributor would reference against the internal database that it created from the information provided by the manufacturer. The Work Group recognized, however, that this approach, which depends upon sending and receiving aggregated product identifier data, could not be widely adopted and implemented by the 2019 enforcement deadline.

2.2 The VRS Task Force

As an outcome of the pilots work, pharmaceutical manufacturers and wholesale distributors formed a Task Force to develop the business requirements and governance associated with the Verification Router Service solution. Working with KPMG LLP and with HDA providing logistical support, task force members conducted several workshops and meetings to collaborate on defining the business requirements and identifying governance needs to oversee and support on-going operation of the complete solution. The task force defined the requirements with the expectation that there will be multiple VRS providers operating in a distributed environment.

The purpose of this document is to provide initial guidance in the form of FAQs to facilitate effective operations and maintenance of VRS solutions across users and solution providers. While the driver behind development of the Verification Router Service is to support the 2019 Saleable Returns Requirements there is the potential for manufacturers to use the VRS to meet other DSCSA requirements that began November 27, 2017 which require them to respond to certain verification requests. There is also potential to include additional future capabilities for expanded use beyond 2023 when full product traceability goes into effect.

This guidance is a first step. HDA currently, and temporarily, receives correspondence, provides administration support of the VRS, and hosts relevant information for dissemination to VRS participants. Trading partners will need to continue to work on the VRS, both to implement it and to assure that the VRS continues to meet business and regulatory needs, ultimately under the auspices of a more formal governing body. HDA does not have any ongoing role in the management or governance of the VRS.

3. Glossary

Term / Acronym	Definition
CI	Connectivity Information, a general term used in this document to refer to the technical information (e.g. end-point URL, security certificates, authentication parameters) needed to establish connection with the responder's repository. The details of what this connectivity information entails will be further defined in the design phase. See the Business Requirements Document (BRD), Lookup Directory (LD) specification and GS1 Lightweight Messaging Standard for Product Verification for more details on use.
DQSA	Drug Quality and Security Act
DSCSA	Drug Supply Chain Security Act, Title II of the DQSA. See full law here or information from the Food and Drug Administration (FDA) here.
FDC Act	Food, Drug and Cosmetic Act. See full law here.
GS1	GS1 is an international organization that develops and maintains standards for supply and demand chains across multiple sectors. For additional information. See here.
GCP	Global Company Prefix, a unique number allocated by GS1 to entities in the supply chain to identify, among other things, location (GLNs) and trade items (GTINs). Within the US pharmaceutical supply chain, GCPs are derived from FDA labeler codes allocated to manufacturers for creation of NDCs. For additional information see here.
GLN	Global Location Number, the GS1 identification key utilized to identify unique physical locations, operational locations, and legal entities. For additional information see here and for healthcare specific GLN information see here. GLNs will be used to identify the Requestor and Responder in the messaging standard.
GTIN	Global Trade Item Number, used to uniquely identify trade items that are priced, ordered, or invoiced at any point in the supply chain. For additional information see here.

Term / Acronym	Definition
NDC	National Drug Code or NDC number is embedded in the GTIN. For additional information on the NDC see here.
UUID	UUID is a universally unique identifier assigned to requests that are initiated within the VRS using 8-4-4-4-12 string format, e.g. 998CDC77-6860-4351-9277-6F3E6F870AC6.
LD	Look-up Directory (directory which contains the connectivity information of the Responder's repository fulfilling the verification request)
PI	Product Identifier, defined by DSCSA as a standardized graphic that includes, in both human-readable form and on a machine-readable data carrier that conforms to the standards developed by a widely recognized international standards development organization, the standardized numerical identifier, lot number, and expiration date of the product. In this context it is used to reference its component data elements which include GTIN, Serial Number, Lot Number, and Expiration Date.
Repository	Repository refers to the Responder's systems that will minimally store the 4 PI data elements and provide the response to the verification request.
Requestors	Entities that will initiate the verification requests (e.g. distributors).
Requestor ID	A unique identifier assigned to Requestor entities that are registered and authorized to use the VRS.
Responders	Entities that will provide response to the verification requests (e.g. manufacturers, re-packagers).
Responder ID	A unique identifier assigned to Responder entities that are registered and authorized to use the VRS.
SNI	Standardized Numerical Identifier, defined by DSCSA as "a set of numbers or characters used to uniquely identify each package or homogenous case that is composed of the National Drug Code that corresponds to the specific product (including the particular package configuration) combined with a unique alphanumeric serial number of up to 20 characters." § 581(20). For additional guidance, though it predates the DSCSA, see here.
Transaction ID	General term for the unique value assigned to requests that are initiated within the VRS. see guide definition.
VRS	Verification Router Service
VRS providers	Solution providers that will provide Verification Router Services

4. Frequently Asked Questions

1. Who can operate and maintain a VRS and LD?

   - Solutions providers as well as individual distributors and manufacturers meeting the minimum requirements outlined in Governance Body Charter and below:

Requirements of VRS Providers to demonstrate qualifications, including interactions with Authorized Trading Partners

Req #	Description
R-001	The VRS Provider shall have the ability to demonstrate a procedure(s) or other documentation that describes the process for verifying authorization of its customers for initiating verification requests; conducting periodic reviews; and documenting the results of this on-going activity.
R-002	The VRS Provider must obtain documented evidence that the wholesale distributor (requestor) is authorized to either distribute or dispense prescription products. Examples of documented evidence include valid/current state license through one of the following methods: obtain a copy of license, confirm with a state licensing board, or use a license aggregator, e.g. MedPro, Atlas Certified, Legisym or other similar. Information may be obtained directly from the entity or using a 3rd party service (e.g. MedPro, Atlas Certified, Legisym or other similar). It is only necessary to verify a single state license to confirm the distributor is "authorized". The license must be active. For states that extend expiration date, grace period needs to be considered If a license cannot be verified, the wholesale distributor should not be allowed access to the system until a valid license can be provided. Note: Neither a DEA license nor the FDA website are valid documentation for this purpose.
R-003	The VRS Provider must obtain documented evidence in R-001 and R-002 with frequency no less than once a month so as to verify that the license is valid and has a non-expired status.
R-004	The VRS Provider must obtain documented evidence that the entity providing Connectivity Information (CI) is the authorized manufacturer responsible for providing responses for the GCP(s)/GTIN(s) identified. Examples of documented evidence could include trusted sources of data (e.g. FDA database, approved product labeling) and/or attestation from manufacturer and co-licensed partner as applicable.
R-007	The VRS Provider will maintain and provide upon request or audit from a customer a listing of all entities for which they are providing requesting and/or responding services. Listing will include, at a minimum, company identifier (i.e. GLN), on-boarding date, contact information, license information, and next review date where applicable.
R-008	The VRS Provider will adhere to published VRS business requirements, specifications and GS1 Lightweight Messaging Standard for Verification of Product Identifiers unless otherwise indicated by VRS Provider.
R-009	The VRS Provider will route verification requests to other VRS Providers as needed based on manufacturer (responder) and wholesale distributor (requestor) solution set/scenario.
R-010	The VRS Provider will make available to other VRS Providers Look-up Directory (LD) information obtained directly from an authorized manufacturer (GCP/GTIN owner).

R-011	VRS providers will make a public statement that they follow the rules as outlined above. VRS providers make public an outline of their ATP check concepts. VRS providers are not required to audit each other but rely on the public statements.
R-012	The VRS Provider and any network participant who intends to provide their own requesting or responding services will utilize a TLS mutual authentication approach, exchanging X.509 certificates. Certificates can either be self-signed or public issued by a certificate authority. Managing certificate validity and expiration dates is something that will need to be taken care of during onboarding between VRS Providers or those building their own requesting or responding services.
R-013	Certificates should have a limited validity of no more than 2 years and a new certificate should be provided at least 90 days in advance of expiry. New and old certificates should be active simultaneously to allow for testing.

2. What information does a company need to provide to operate/maintain a VRS & LD?

➢ To operate and maintain a VRS and LD, a company will need to collect [or obtain?] and maintain the following information for assignment of a VRS ID, general communication purposes, and administration:

VRS_ID*	Company Name	Company Address	Contact Name, E-mail, and Phone
VRS1nn			

*VRS_ID value is assigned at the time the company is added to the registry of solution providers; nn = integer value; a new provider would be assigned the next available number, e.g. a new provider who is 9th on list would be assigned VRS109 as their VRS_ID. This value is relevant for the synchronization of LD records.

3. How does a VRS/LD provider communicate the minimum required information indicating that it will operate and maintain a VRS/LD and to whom should this information be communicated?

➢ Solution providers and any company intending to provide their own requesting or responding services should notify each other of their intent to operate and maintain a VRS/LD until a governance body is established. A list of solution providers can be found at https://hdma365.sharepoint.com/sites/vrs/Shared%20Documents/Forms/AllItems.aspx. Once a governance body is established, correspondence will be directed to the governance body. For assistance until a governance body is

established, correspondence may be directed to:
VRS@hda.org

4. How are additions/changes to VRS/LD provider network communicated/made known?

    ➢ Until a governance body is established to administer the VRS, HDA is temporarily hosting an updated registry of providers at the following location:

    https://hdma365.sharepoint.com/sites/vrs/Shared%20Documents/Forms/AllItems.aspx

    ➢ VRS/LD provider contact information is included in the registry to facilitate direct communications between companies if/as needed.

5. How is security between VRS/LD providers managed?

    ➢ Refer to the document located here:

    https://www.hda.org/~/media/pdfs/industry-relations/vrs-documents/2019/vrs-current-security-approach.ashx

6. How is security between a VRS/LD provider and its individual customers/users maintained?

    ➢ A detailed approach for how distributors, manufacturers, and their respective solution providers should manage security between their customers was not in scope of the VRS task force. It is the responsibility of each VRS/LD provider to implement appropriate controls and align with its customers on security protocols. Some high level requirements on Authorized Trading Partners were put together and can be found here: https://www.hda.org/~/media/pdfs/industry-relations/vrs-documents/2019/vrs-authorized-trading-partner-requirements.ashx

    ➢ A high level security approach was put together for security between solution providers. Solution providers and network participants who intend to provide their own requesting or responding services are currently utilizing a mutual authentication approach exchanging X.509 certificates. Certificates can either be self-signed or issued by a public certificate authority. Certificates are exchanged on a one-to-one basis with entities listed in the Registry (at a minimum) so that all entities are known to everyone else in the network. Managing certificate validity and expiration dates must be addressed during onboarding between solution providers or those building their own requesting or responding services.

7. How does a manufacturer establish that it is responsible for responding to a request to verify a PI for a given GTIN?

    - ➢ The FDA labeler code can be used to validate the entity uploading an LD record. The FDA labeler code registry is one mechanism available to determine the responsible organization as the GTIN is based off of the product’s NDC code. LD Providers are expected to take appropriate measures to verify the integrity of the data provided to them by manufacturers.

    - ➢ The LD Sync Specification outlines the fields required for a manufacturer to provide information on each GTIN, as well as the use cases for publishing or broadcasting updates. The manufacturer will attest to the completeness and accuracy of the connectivity information (CI)it provides for each GTIN uploaded to one or more of the LDs.

8. Can more than one manufacturer respond to verification requests for the same GTIN? What are the restrictions/limitations?

    - ➢ Yes, there could be business scenarios where there will be more than one active entry, that is, responding manufacturer, in an LD for the same GTIN. While multiple companies can respond for the same GTIN, only one company can respond for the combined unique four pieces of information that make up the product identifier. In order to accurately route verification requests to the appropriate responder, the expiration date value of the PI must be assessed against the startExpDate and endExpDate values in an LD. The fields startExpDate and endExpDate are the parameters used to determine the appropriate repository. Therefore, there is a restriction that if multiple entries exist in an LD for the same GTIN, the startExpDate and endExpDate values cannot overlap, i.e. the startExpDate value for the second LD record must be greater than the endExpDate value of the first LD record. For more details on fields and use cases, see the LD synchronization specification.

9. How does a manufacturer responsible for a GTIN indicate via interaction with an LD that it is granting authority of another manufacturer to respond to verification requests for that same GTIN?

- The manufacturer responsible for the GTIN will need to update two of the fields in an LD for the impacted GTIN:

  1. endExpDate – it is likely that this value was initially NULL and will therefore need to be updated with an actual date to delineate a change in responsibility for responses. This value will be used to validate that the startExpDate of the second LD entry for the GTIN does not overlap with the first LD entry. Two companies cannot both be responding to verification requests for the same GTIN within the same startExpDate and endExpDate parameters.

  2. nextRecordOwner – the manufacturer initially responsible for the GTIN, a.k.a. the LD record Owner, must indicate the FDA Labeler code of the next record owner. This value will be used to validate the entity uploading an LD record for a GTIN which already exists in the LD.

10. How is start/end ExpDate values in an LD used to logically identify the party responsible for responding to a verification request for a particular GTIN?

    - endExpDate: when this value is NULL, the nextRecordOwner value cannot be accepted and therefore a second entry to the LD is not possible for the same GTIN.

    - startExpDate: this value indicates the starting expiration date value for which manufacturer will be responsible for providing responses to verification requests as of a certain, identified date. This value must be after the endExpDate of the previous record owner (manufacturer).

11. What are the potential response options for a verification request?

- The GS1 Lightweight Messaging Standard for Product Verification can be found at https://www.gs1.org/verification-messaging. A guideline is underway which will further explain how to implement the standard. Below are the potential response options and how to utilize the additionalInfo field.

Scenario Number	Scenario Description	verified	verificationFailure Reason	additionalInfo
Scenario 1	Product Identifier matches AND Manufacturer has no additional info to share	true	n/a	<not provided>
Scenario 2	Product identifier matches but Manufacturer has Recall info to share.	true	n/a	Recalled
Scenario 3	Product Identifier matches but Manufacturer has reason to believe product is suspect.	true	n/a	Suspect
Scenario 4	Product Identifier does NOT match and Manufacturer provides no reason for verification failure	false	No_reason_provided	<not provided>
Scenario 5	Product identifier does NOT match and Manufacturer provides a reason for verification failure	false	One of the following can be provided: No_match_GTIN_Serial No_match_GTIN_Serial_Lot_Expiry No_match_GTIN_Serial_Lot No_match_GTIN_Serial_Expiry	<not provided>

*Each individual business will determine what action it will take based upon its own requirements and judgments.   The above is not intended to suggest how all businesses must respond.

- For scenario where PIs do NOT match, in column B (verificationFailureReason), the manufacturer can choose to indicate any of the current 5 options for verificationFailureReason enumeration list ("No_match_GTIN_Serial", "No_match_GTIN_Serial_Lot_Expiry", "No_match_GTIN_Serial_Lot", "No_match_GTIN_Serial_Expiry", “No_reason_provided”).
- For scenario where the PIs match but a manufacturer has recall info to share, the manufacturer should provide ‘No_reason_provided’ as the verificationFailureReason because the other 4 reasons ("No_match_GTIN_Serial", "No_match_GTIN_Serial_Lot_Expiry", "No_match_GTIN_Serial_Lot", "No_match_GTIN_Serial_Expiry") do not apply since the premise of the scenario is that PIs are matching.
- For scenario where PIs match but a manufacturer has reason to believe that product is suspect- Column C (additionaInfo) is highlighted because the workgroup is requesting GS1 add “Suspect” as a new value in the additionalInfo enumeration list.

12. What conditions in an LD might indicate than an update is pending or expected?

   - When the current record owner updates an LD with a value for endExpDate and nextRecordOwner, it is anticipated that a second LD entry for the GTIN will be made by the manufacturer (FDA Labeler code owner) indicated as the nextRecordOwner.

13. How is FDA Labeler Code used to verify GTIN entries and updates in an LD?

   - See FAQ #7

14. Who is responsible for providing or uploading CI to an LD?

   - The manufacturer who owns the marketing authorization for the GTIN is responsible for providing and uploading CI to an LD. The manufacturer can delegate this responsibility to another manufacturer (e.g. co-license partnership, divestiture of GTIN) by leveraging the endExpDate(FAQ #9) and nextRecordOwner (FAQ #11) fields of the LD. See FAQs #9-#11.

15. Who is responsible for ensuring that the PI data of GTINs are staged in a PI repository in a timely manner?

   - The manufacturer [or its designee?] who owns the marketing authorization for the GTIN is responsible for uploading PIs assigned to its products and maintaining and updating that repository.

16. Will all GTINs be entered in an LD?

   - No. Not all products are in scope for re-stock/re-sale even if the PI were to be verified. The determination of which products are in scope of the LD is the responsibility of the manufacturer.

17. What additional information do manufacturers need to provide to participate in the VRS?

   - VRS solution providers are expected to request appropriate documentation/attestation from their manufacturer customers indicating authority for providing responses for each GTIN uploaded to an LD. VRS solution providers can use FDA Labeler Code/GS1 GCP to verify multiple GTINs.

18. What information do Requestors (distributors) need to provide to participate in the VRS?

    - ➢ VRS solution providers are expected to request appropriate documentation/attestation from their distributor customers indicating authority to generate Verification Requests. A State Board of Pharmacy license would be an example of appropriate documentation.

19. Can a manufacturer participate in the VRS if it chooses to build and manage its own PI Repository and responses to verification requests?

    - ➢ Manufacturers who choose to build and/or manage their PI Repository and verification responses will need to provide their CI either to a VRS solution provider (for replication to all other LDs) or provide their CI directly to distributors for whom they want to provide responses for verification requests.

20. What actions should a Requestor take when it wants to receive verification responses from a manufacturer that has built and/or is managing its own system for verification of its PIs?

    - ➢ Manufacturers who choose to build and/or manage their PI Repository and verification responses will need to either obtain LD records from a VRS solution provider or directly from manufacturers to whom they want to send VRs.

21. Is there planned downtime for VRS/LD solutions? What is the expected frequency/schedule?

    - ➢ Yes. The frequency and schedule is still to be determined.

22. Are releases planned for VRS/LD functionality? What is the expected frequency/schedule?

    - Yes. The frequency and schedule will be determined, however, it is likely that the to be established governance body would release upgrades at least annually, being mindful of the frequency and impact to companies.

23. How does an individual VRS/LD provider indicate to all other companies operating/maintaining VRS/LD on the network that it is going to cease operations? What information is required?

    - Solution providers should send an e-mail communication to all contacts listed in the registry providing the planned termination date. The communication should be sent with sufficient lead time, ideally at least 6 months prior to the planned termination date.
    - It is the responsibility of the solution provider to work with both their current customers, as well as other solution providers, to manage transition activities and timing.

24. Who do I contact with issues, questions, or suggestions?

    - Until a governance body is established contact HDA at VRS@hda.org.

25. Do I need a GLN for VRS?

    - Yes, a GLN is required for the VRS. It is a component of the messaging standard. To obtain a GLN, contact GS1. For more information on how GLNs are utilized in healthcare, see the Healthcare GLN Implementation Guideline.

26. Will the VRS be used for other types of verifications than saleable returns?
    - The VRS was designed for the purpose of verification of saleable returns. Some members of the Work Group envisioned that the VRS might prove sufficiently robust to support other types of verification in the future.