HDA
Healthcare Distribution Alliance
PATIENTS MOVE US.

March 29, 2018

BY ELECTRONIC FILING
http://www.regulations.gov, Dkt. No. FDA-2017-N-3857

Connie T. Jung, R.Ph., PhD
Senior Advisor for Policy
Office of Drug Security, Integrity, and Recalls
Office of Compliance
Center for Drug Evaluation and Research
Food and Drug Administration
Room 2242, White Oak Office Building 51
10903 New Hampshire Avenue
Silver Spring, MD 20993
connie.jung@fda.hhs.gov

RE: Enhanced Drug Distribution Security Under the Drug Supply Chain Security Act; Public Meetings; Request for Comments, 82 Fed. Reg. 33505 (July 20, 2017), Dkt. No. FDA-2017-N-3857, Comments to February 28, 2018 Public Meeting.

Dear Doctor Jung:

The Healthcare Distribution Alliance (HDA) appreciates this opportunity to provide comments to the Food and Drug Administration (FDA) regarding the public meeting on February 28, 2018 in connection with Enhanced Drug Distribution Security under the Drug Supply Chain Security Act; Request for Comments, 82 Fed. Reg. 33505 (July 20, 2017), Dkt. No. FDA-2017-N-3857 ("Request for Comments").

HDA represents primary pharmaceutical distributors – the vital link between the nation's pharmaceutical manufacturers and more than 200,000 pharmacies, hospitals, long-term care facilities, clinics and others nationwide. This essential function is provided with little public recognition or visibility, and at great savings to the healthcare system. HDA members serve as the central link in a sophisticated national supply chain. HDA members take this mission very seriously, and we support manufacturers, healthcare providers, and the government in ongoing efforts to ensure the U.S. medicine supply remains secure, efficient, and highly regulated.

I. OVERVIEW

HDA appreciates the public meetings FDA has sponsored and the opportunities for participation and comment on enhanced security under the Drug Supply Chain Security Act (DSCSA). HDA staff and its members who participated all considered the most recent, February 28 public meeting to be productive and useful. We were particularly grateful for Commissioner Gottlieb's opening remarks and engagement on the DSCSA. We welcomed the announcement of the release of the two guidances and the Commissioner's recognition that fragmentation of state licensing regimes was one of the security vulnerabilities Congress sought to address in the DSCSA. We eagerly await this reexamination of FDA's interpretation of § 585 of the federal Food, Drug and Cosmetic Act set forth in the October 2014 draft guidance[1] as well as the federal licensure standards currently identified in the Agency's regulatory agenda for release in June 2018. We noted and appreciated that FDA appeared to more aggressively focus the public meeting on topics within the scope of the DSCSA's requirements and thereby supported a more productive discussion.

We offer comments below on the following two issues:

- We discuss certain components of the 10-points on "Enhanced Security Needs" that FDA disseminated in advance and during the public meeting. HDA has previously urged greater appreciation for and recognition of the "distributed model," including its contributions to overall supply chain security and its critical importance as a necessary building block to greater functionalities. We appreciated the fact that during the 10-point discussion and elsewhere during the meeting, there was also an opportunity to hear from stakeholders well in advance of the 2019 deadline requiring wholesale distributors to verify the product identifier on products prior to their resale. We reiterate these issues again, and further address both attributes of the 2023 Enhanced Security Needs and interpretations of the DSCSA's verification of saleable returns directives.

- With regard to FDA's request for more information on where and how the Agency might aid DSCSA implementation, we offer suggestions for where FDA concurrence would be useful.

II. ENHANCED SECURITY NEEDS

In advance of and during the February 28 public meeting, FDA discussed 10 Enhanced Security Needs intended to improve the ability of the supply chain to identify and help prevent the distribution of suspect or illegitimate product:

1. Fully electronic and interoperable
2. Secures data and system(s) against falsification, malicious attacks and breaches
3. Ensures the protection of confidential commercial information and trade secrets

[1] See the draft guidance "*The Effect of Section 585 of the FD&C Act on Drug Product Tracing and Wholesale Drug Distributor and Third-Party Logistics Provider Licensing Standards and Requirements: Questions and Answers*."

4. Enables authorized trading partners to capture, maintain and exchange data accurately and efficiently for each transaction
5. Enables the prompt response of the transaction information (TI) and transaction statement (TS) for product upon request by the FDA (or other appropriate Federal or State official) in the event of a recall or for purposes of investigating a suspect product or an illegitimate product
6. Facilitates prompt gathering of the information necessary to produce the transaction information for each transaction going back to the manufacturer, when requested by the FDA (or other appropriate Federal or State official) in the event of a recall or for purposes of investigating a suspect or illegitimate product
7. Enables authorized trading partners to verify product identifiers accurately and efficiently to facilitate investigations of suspect or illegitimate product, recalls and saleable returns
8. Signals that a product has been determined to be illegitimate (e.g., red flags)
9. Enables scalability for integration by any size business
10. Prevents trading partners who are not "authorized" from accessing and using the system

We offer comments below on points 1-3, 5-8 and 10. We have no further comments on elements 4 and 9 and support their inclusion in this list of Enhanced Security Needs.

Point 1 – Fully electronic and interoperable

Overall, we continue to be concerned with the apparent assumption and, in many instances, the direct statements that the enhanced security needs for 2023 must be met with a ***single*** system that should be able to perform ***all*** DSCSA functionalities, including:

- Confirm authorized trading partner status;
- Receive, hold and transmit transaction data;
- Conduct verification processes for saleable returns and in suspect product investigations; and
- Alert the entire supply chain of a suspect product or other product problem, such as a recall.

Wholesale distributors already have business processes in place to conduct many of the activities the DSCSA requires; the processes often predate the DSCSA, such as processes for conducting supplier and customer due diligence and for identifying and notifying customers who purchased recalled product. We believe the DSCSA's directives were intentionally layered into these existing processes to avoid, as much as possible, unnecessary disruption to the supply chain as well as unnecessary expense. We expect that the additional functionalities that will eventually arise with the DSCSA, such as item-level serialization, transmission and capture of serialized data and interoperable point-to-point data exchange between trading partners, will ultimately enhance and improve these processes.

HDA believes that a fully integrated, single system is not possible at this time. Nor do we believe it is mandated in the law. To the extent that FDA envisions a more consolidated system, nothing that is being done today precludes movement to adding additional functionality in the future, as technologies mature.

Recommendation: HDA urges FDA to recognize that there will not be a single "catch-all" system for compliance with all DSCSA requirements effective as of 2023. Rather, we urge the Agency to continue to work with stakeholders to support compliance with the DSCSA's multiple requirements using the processes and systems that are already in use and that supply chain stakeholders are developing.

Point 2 – Secures data and system(s) against falsification, malicious attacks, and breaches

HDA agrees that each authorized trading partner must take appropriate measures to assure that its data and systems are protected and secure. However, given the rapid changes in data and system security and the need for rapid responses to threats as they arise, we do not believe that FDA would be able to provide useful guidance in a timely manner. Wholesale distributors are also particularly concerned that in-depth discussions of security information and requirements could inadvertently provide a "road map" that criminals or "hackers" could use to more easily determine how to breach trading partners' data repositories and internal systems with the express purpose of exploiting data.

Recommendation: Given FDA's scarce resources, the very protective data security methods and expertise already being utilized in the pharmaceutical industry and the critical need to maintain privacy of security practices, HDA does not believe that further elucidation of data and system security should be a priority for FDA. The supply chain is highly motivated to secure their own valuable data and protect against intrusions.

Point 3 – Ensures the protection of confidential commercial information and trade secrets

HDA agrees that any enhanced security system should assure that each trading partner's confidential commercial information and trade secrets remain protected. Moreover, § 582(g)(1)(E) assumes that requests for TI in suspect and illegitimate product investigations must consider and protect a trading partner's confidential information and trade secrets. However, we do not interpret this provision as suggesting that one trading partner has end-to-end supply chain visibility into another trading partner's purchases or sales.

Recommendation: HDA urges FDA to recognize that § 582(g)(1)(E) does not force a trading partner to share all its highly confidential purchase and sale data; rather, this section provides a mechanism for protection of confidential information in the event of an investigation or recall that requires disclosure of confidential customer or supplier information.

<u>Point 5</u> – Enables the prompt response of the TI and TS upon request by the FDA (or other appropriate Federal or State official) in the event of a recall or for purposes of investigating a suspect product or an illegitimate product

From the public meeting, it appears that FDA may be interpreting "prompt response" to mean that, upon receiving an appropriate request, a trading partner is able to produce TI and TS for a product transaction in near real- time. We caution that the internal systems trading partners will use to manage transaction data and the point-to-point connections necessary to receive and transmit data and the standards associated with those data exchanges, are still under development. Still, HDA believes that it is reasonable to expect that once trading partners are transacting in serialized product and receiving and sending serialized data, each trading partner should be able to draw from its internal systems, by product identifier, the TI and TS it received for a product and the TI and TS it transmitted for a product. We believe systems should be, and in fact are, being developed to provide this level of swift response and functionality.

We caution that in the distributed-model that has been discussed, and that we believe the DSCSA contemplates, each trading partner maintains its own data and can only maintain and produce the transaction data it has received and sent. Therefore, one trading partner will not, for instance, have visibility into a downstream customer's subsequent sale of the product.

Recommendation: We urge FDA to support the systems currently under development that will enable a trading partner to query and produce the transaction data it has received, maintained and sent in order to promptly respond to appropriate requests.

<u>Point 6</u> – Facilitates prompt gathering of the information necessary to produce the transaction information for each transaction going back to the manufacturer, when requested by the FDA (or other appropriate Federal or State official) in the event of a recall or for purposes of investigating a suspect or illegitimate product

HDA notes first that § 582(g)(1)(E) specifically states that a trading partner must have "systems and processes necessary ***to promptly facilitate gathering*** the information necessary to produce" the TI for each transaction going back to manufacturer, as applicable (emphasis supplied). The statute does not state, as quoted in Point 6 of the 2023 Enhanced Security Needs, that the contemplated system(s) must "facilitat[e] prompt gathering of the information necessary. . .". ***Facilitating*** the gathering of the information must be done promptly, not the gathering of the information.

FDA repeatedly emphasized at the public meeting that, while TH sunsets pursuant to § 351(k) in 2023, this historical information is important and "doesn't go away." HDA agrees. To elaborate, in the distributed model for 2023 where each trading partner retains its own data, a trading partner will only have and only be able to provide the data that it received from its selling trading partner and the data it generated in its sale to its customer. A product's full sales history is available, but it will not reside in one place because the trading partner did not receive it.

Further, it seems that a belief continues to persist that transaction data should operate as a continually updating document attached to a single product – similar to a delivery service's (*e.g.*, UPS or FedEx) tracking method that updates information as product moves in transit. (We note that such delivery systems do not track the manufacture of the item in the box, nor is it tracking whether the buyer resells the item in the box). The DSCSA, however, is built upon a structure where each trading partner holds its own purchase and sale data and promptly produces what it has about a product upon request.

The Advance Ship Notice (ASN) transaction set, in use now, and the Electronic Product Code Information Services (EPCIS), which we believe most supply chain members will use to satisfy DSCSA data transmission requirements in 2023, are generated anew with each change of ownership (and in the case of EPCIS, are also associated and generated with other product events). These electronic transactions and events do not follow a single product through the supply chain, continually updating with each change or event.

Additionally, in prior comments HDA has provided a detailed explanation of our interpretation of a trading partner's responsibilities in 2023 to maintain data and produce that data when an appropriate official requests it.[2] The analysis contained in our prior comments is consistent with the above point – the DSCSA does not require or even contemplate that a single trading partner must have visibility into, or produce upon request, another trading partner's data beyond what was explicitly generated in a transaction between those two trading partners. We incorporate those comments by reference into this docket, as well.

Recommendation: We urge FDA to recognize that when the Agency (or other appropriate official) requests that a supply chain entity provide data under § 582(g)(1)(E), the entity will promptly produce and provide the data that it has, which will be for that entity's transactions with its immediate selling and purchasing trading partners. The supply chain entity will not produce data that it does not have in its possession and that the DSCSA does not require it to obtain or maintain pertaining to all transactions for that product.

<u>Point 7</u> – Enables authorized trading partners to verify product identifiers accurately and efficiently to facilitate investigations of suspect or illegitimate product, recalls, and saleable returns

There was much discussion at the public meeting regarding verification. There was consensus that the DSCSA's enhanced security requirements included the need to verify product identifiers and the ability to verify a product's identifier in response to a request from a direct trading partner that is authorized. There was not consensus regarding whether a manufacturer must respond to a verification request made by an authorized trading partner that it did not directly sell product to.

[2] See comments of HDA to Dkt. No. FDA-2016-N-2673, https://www.regulations.gov/document?D=FDA-2016-N-2673-0010, submitted November 14, 2016.

Section 582(b)(4)(C) provides:

> upon receiving a request for verification from an authorized repackager, wholesale distributor, or dispenser that is in possession or control of a product such person believes to be manufactured by such manufacturer, a manufacturer shall, not later than 24 hours after receiving the request for verification or in other such reasonable time as determined by the Secretary, based on the circumstances of the request, notify the person making the request whether the product identifier, including the standardized numerical identifier, that is the subject of the request corresponds to the product identifier affixed or imprinted by the manufacturer.

We do not interpret § 582(b)(4)(C) as permitting ***only*** those authorized trading partners that purchased the product directly from a manufacturer to make a verification request to that manufacturer. We say this because § 582(b)(4)(C) appears to permit any "authorized" repackager, wholesale distributor or dispenser in possession or control of a product to make a verification request. There are no further qualifiers placed on who may make the request, including no restrictions stating that the requesting entity must be a direct trading partner. Similarly, the term "Authorized" as defined in § 581(2), contains requirements for licensure and/or registration; the definition is not limited only to entities that have purchased directly from a seller.

Recommendation: We recommend that FDA clarify its interpretation of this requirement. HDA further urges FDA to clarify that its reading of § 582(b)(4)(C) is that if a repackager, wholesale distributor or dispenser is authorized and in possession or control of a product, the manufacturer shall respond to the request for verification.

<u>Point 8</u> – Signals that a product has been determined to be illegitimate (e.g., red flags)

HDA acknowledges and agrees that the DSCSA imposes upon trading partners the duty to notify other trading partners of illegitimate product, of product subject to recall, and in suspect product investigation, all under the conditions set out in the statute. As previously discussed and as presented at the public meeting, we believe trading partners intend to continue to use existing methods for communicating with other trading partners about product problems, such as e-mail, portals and fax. In the absence of any demonstration that current practices are inadequate or not legally compliant, and with no financial or operational support, we do not see compelling business, compliance, or safety pressure for the supply chain to change these current methods of communicating product problems.

We have discussed previously our concerns regarding suggestions that these notification practices to trading partners should be expanded to a "Sentinel-like" signaling that disseminates "red flags" throughout the pharmaceutical supply chain about potential product problems. Practically speaking, such a system would seem to presuppose the creation of a national communications network that linked all members of the pharmaceutical supply chain to one another. We do not see a mandate for creation of such a centralized notification system in the DSCSA and anticipate significant practical hurdles as well.

Further, given the complexity in simply standing up and operationalizing a point-to-point connection between an individual wholesale distributor and each of its hundreds or thousands of dispensing customers in order to pass transaction data, we do not believe execution of a nationwide alert system by 2023 is feasible. And if, as it appeared from the discussions, FDA's expectation is for a single communications system whereby thousands of manufacturers would signal to hundreds of wholesale distributors who would signal to hundreds of thousands of dispensers, we believe the cost and complexity render such a system wholly impractical – and would, we believe, impede efforts to comply with other, express DSCSA requirements. Further, for such a system to have the benefits envisioned, it would seem to require dispensers to scan products at time of dispensing to determine if the product is legitimate and still appropriate for dispensing – not a responsibility the DSCSA imposes.

Though we do not see the need to change the mode for communicating recalls, the greater specificity that product identifiers and serialized data provide will likely change the content of recall communications and make them clearer and more effective in 2023 and beyond. Better targeting and specificity may mean fewer, but more impactful, notifications. Suspect product investigations and illegitimate product notifications to trading partners have not, in the experience of wholesale distributors, yet been so common as to warrant drastic changes to existing communications processes. Wholesale distributors have developed business processes and standard operating procedures for addressing these matters swiftly with impacted trading partners.

Recommendation: Current requirements already obligate trading partners to have systems and processes for informing other trading partners of product problems. Therefore, HDA recommends that FDA delete Point 8 of the Enhanced Security Needs. The statute does not require an active surveillance system or compel dispensers to scan products prior to dispensing, which would be necessary for such a surveillance system to have any meaning or utility.

<u>Point 10</u> – Prevents trading partners who are not "authorized" from accessing and using the system

We discussed above the lack of consensus regarding the manufacturers' obligations to respond to verification requests made by authorized supply chain entities that the manufacturer did not sell directly to, such as request made by a dispenser or a secondary wholesale distributor. While we believe that the DSCSA permits an indirect purchasing supply chain member who is "authorized" to request that a manufacturer verify a product identifier, we recognize there are differing views. We suggest that FDA consider this issue further and advise industry of its interpretation of § 582(b)(4)(C).

We also addressed previously our continuing concern with characterizing the 2023 model as "the system" when stakeholders have assumed FDA concurs with their views in development of a distributed model where each trading partner retains control of its own data. As such, while unauthorized access to a trading partner's transaction data and its repository of product identifiers (if

it has one) pose serious concerns, these are matters of internal security that each trading partner must address individually within its own organization.

HDA notes that the term "authorized" as used in Point 10 of the Enhanced Security Needs could be confused with the term "Authorized" defined in § 581(2). It appears that in Point 10, the Agency meant to indicate that there should be a form of approval or permission for someone to access a database and/or a system. We do not believe it was intended to mean that the system would somehow block out anyone who was not defined under § 581(2) yet allow *anyone* who *is* defined as "authorized" (licensed, registered) under § 581(2) to access it. In the distributed model, each trading partner expects to maintain access to its own data and we do not expect that, as a routine matter, one trading partner will have access to another's database or system. Trading partners would be expected to take extreme care to limit *any* access, including access even by their own employees, to the bare minimum to help prevent hackers and other unwanted individuals from attempting to breach their systems.

Recommendation: We urge the Agency to recognize that a distributed model will provide greater security assurance than will a single system. We also urge recognition that each entity in a distributed model will maintain its own methods for approving or permitting access that is consistent with a distributed model. Finally, we suggest that FDA reword Point 10 to omit use of the term "authorized" to avoid confusion with this term and its specific meaning/definition in § 581(2).

III. IDENTIFICATION OF WHERE ADDITIONAL FDA SUPPORT AND GUIDANCE WOULD BE USEFUL TO DSCSA IMPLEMENTATION

During the public meetings, stakeholders have frequently requested that FDA provide "guardrails." Rather than attempting to define what guardrails are and mean, HDA suggests specific areas where FDA's explicit support and affirmation would be useful to DSCSA implementation:

- Recognition that in 2019, the inability to immediately verify a product identifier does not automatically mean the product is "suspect" pending further investigation.
- Permit the use of Master Data in lieu of transmitting the same, static data with each transaction.
- Affirm that a serialized GTIN plus lot and expiration date, in conformance with GS1 standards, is the preferred product identifier.
- Affirm the use of aggregation and inference and confirm that it may be used to meet 2023 data exchange requirements.
- Clarify what parameters of DSCSA compliance are subject to current Good Manufacturing Practices, 21 C.F.R. Parts 210 and 211 (GMP) and which are not. We urge clarification that internal processes such as processes for assigning serial numbers, storing that data, and labeling product with that number on packaging lines, are subject to GMPs. However, once the product identifier is assigned and the product is labeled, we urge FDA to clarify that subsequent data and transactional processes are not subject to GMP regulations. Specifically, we urge recognition that errors in aggregation of assigning individual product serial numbers to a larger unit serial number such as a case

(also referred to parent/child relationships), are trade and transactional concerns, not GMP issues.

- Acknowledgment that a "distributed" model is acceptable in 2023.
- Express recommendation for and endorsement of GS1 standards suites.

* * *

HDA thanks FDA for this opportunity to comments and suggestions on FDA's February 28 public meeting. If you have any questions, please contact me at 703-885-0240 or at aducca@hda.org.

Sincerely,

Anita T. Ducca
Senior Vice President, Regulatory Affairs