Recommendations for FDA Track-and-Trace Pilots

By Jeff Stollman, Rocky Mountain Technical Marketing, Inc.

Based on the feedback obtained during the FDA's recent public meetings, in combination with our own specialist knowledge of supply-chain-integrity solutions, we make the following recommendations to the FDA and members of the pharmaceutical supply chain for pilots to support the track-and-trace provisions of the Drug Supply Chain Security Act (DSCSA).

The industry is currently struggling with answering a burning and divisive question: What is the best model for a compressive track and trace system required by DSCSA. Industry members fall generally in to two camps. One favors a centralized solution. The other favors a decentralized model. This deadlock can best be resolved by running parallel pilots of each models. These pilots can then be used to test the two critical questions that divide the two camps: :

1. Can either (or both) model provide the full scope of capabilities required by DSCSA?
2. Can either (or both) model protect the highly valued proprietary sales data that is required to facilitate that FDA's mission.

We recommend that each of these questions be addressed separately as described below.

Pilot 1: Functionality Proof of Concept

Because the industry is divided on the question of whether the best solution is a decentralized solution or a centralized solution, the most important pilots would be proofs of concept for both the decentralized and centralized models[1]. Piloting solutions for both models would demonstrate whether either (or both) are capable of meeting the objectives of DSCSA in a practical manner.

We summarize the features of both Functionality Proof of Concept pilots below:

1. Both pilots should demonstrate the following high-level objectives:
    a. The ability of the FDA to track a product up the supply chain to its source
    b. The ability of the FDA to trace the dissemination of a group of products
    c. The ability of a manufacturer to issue a product recall to all inventory holders in the supply chain.

[1] We recognize that there is actually a third alternative available to the industry. We believe that the blockchain solution advocated in a previous submission to the FDA docket. The blockchain solution is a form of centralized solution that offers advantages in functionality, performance, and security. Accordingly, the industry may be best served by the development of a third pilot to address this third solution alternative.

    d. The ability of any member of the supply chain(especially dispensers who are the farthest from the manufacturing source) to verify the provenance of a product.
2. In addition to meeting these high-level objectives, the pilots should allow for the determination of the performance of each approach. These measures are necessary to determine both statutory and practical performance, including:
    a. The ability to calculate elapsed time to obtain a complete report for each of the objectives listed above
        i. Stress-testing. The ability to calculate elapsed time to obtain a complete report at scale which would include approximately 4 billion saleable products produced per year transiting through approximately 3 transactions each for the life of the product (Because there is limited decommissioning required of the system, serial numbers may be kept life as long as the product is being produced and sold.)
    b. The ability of the FDA to deal obtain access to thousands of trading partner systems without having to follow unique access control procedures for each one.
    c. The ability to maintain data integrity through an extended testing period with many transactions.
3. The pilots should demonstrate the ability to meet these objectives for a variety of use cases that include, but are not limited to:
    a. packaging provided by third-party logistics
    b. repackaging of product
    c. drop shipment of product
    d. investigational drugs
    e. 340B
    f. reconciling over/under shipments
    g. data transfer using EDI
    h. data transfer using EPCIS
    i. the system's ability to adapt to a trading partner going out of business
    j. the system's ability to facilitate the discovery of suspicious products
        i. This can be done using synthetic data in order not to introduce actual counterfeit products into the supply chain.
    k. The ease (including cost) of implementing the system for trading partners of varying size and complexity
        i. Cost estimates should be developed to capture both implementation costs and ongoing operational costs including
            1. systems management
            2. database management
            3. access management
            4. security
            5. tech support
    l. The ability of the system to control access
    m. The ability of the system to support aggregation at multiple levels

n. The ability of the system to address packaging systems that cannot provide 100% confidence in the serial numbers contained within a carton or pallet

4. The pilots should also be tested with other use cases referenced during the FDA meetings, but not explicitly articulated into use cases, such as
    a. inference
    b. redaction
    c. other (TBD)

Pilot 2: Data Security Proof of Concept

A second critical demonstration should highlight the robustness of the system in its ability to protect proprietary sales data because this is such an important issue to the industry. This pilot should be performed by retaining a national respected security firm to perform ethical hacking to demonstrate the robustness of the approach.

Assuming that both of the above pilots can prove viable, we again recommend two sets of pilots to demonstrate this ability: one for each of the two models. The purpose here is not to demonstrate that each model is impenetrable. As any security expert will testify, perfect security cannot be attained. But we can obtain some data on the relative difficulty of penetrating each model to determine if one is, indeed, more vulnerable than the other.

Because 100% security is not achievable, the goal of this pilot will be a comparative assessment of the time and effort required to obtain access to data in the decentralized enterprises or the centralized solution that exposes any of the following:

1. the identity of trading partners (suppliers or customers) for particular transactions
2. the quantities of particular products received and/or shipped

In addition, the contract with the security firm performing this work may also include an audit of security processes and assessment of their ability to prevent the exposure of data through human error.

The Data Security Proof of Concept should be constructed as follows:

1. For the centralized model, we recommend using the pilot already developed above to demonstrate feasibility and performance.
2. For the decentralized model, a different approach is required. Because, in the decentralized model , each trading partner maintains its own data, the robustness of the solution is actually a measure of the robustness of each trading partner's own security. We can, therefore, measure the robustness of such a solution by measuring the robustness of each trading partner's system. But measuring thousands of systems is not feasible. Furthermore, a benefit of the decentralized model is that a breach of a small company's system does not necessarily imperil the data held by a larger trading partner with more data at stake and with more robust security controls.

   a. Because no system is 100% secure and no company wants to have a breach of its system made public, we recommend that a dozen or more of the industry's strongest firms participate in the security robustness pilot.
   b. The attack would then be launched against three or four of them selected at random. The names of those attacked would never be disclosed. This sampling would give a strong indication of the robustness of the decentralized model, while providing full reputational cover to all firms involved in the pilot. Each trading partner would retain plausible deniability that their IT infrastructure had been successfully hacked.
   c. The selection of firms for the process audit need not be the same as for the ethical hacking test. If the process audit is included for decentralized firms, the firms audited would have to agree on the audit because it will be invasive to their daily business. The name of firms audited need not be disclosed in the report on the process audit.
3. In the end, a comparison of the vulnerabilities of each model may prove persuasive.
   a. We recognize that firms with strong IT will NEVER favor pooling their data in a shared system. These firms will prefer to address their own vulnerabilities rather than leave their data in the care of a third-party custodian.
   b. But should the centralized model demonstrate security at least as robust as that of the industry's strongest firm, the FDA can judge the prudence of driving the industry towards a centralized solution.