DSCSA Pilot for Kit Check and Sandoz

Final Report

Submitted to the FDA by Kit Check on February 28, 2020

Prepared by Tim Kress-Spatz and partners

Introduction 3

Part 1 - Technical Primers and Background 5
RFID Tags 5
Master Data Repository 7
Modern Cloud-based Software Architecture 7
Single Source of Truth 7
cGMP in the Cloud 8
System Security, Reliability, and Accuracy 9
Barcodes vs RFID Tags 9
Blockchains 11

Part 2 - Pilot Evaluations and Findings 13
Identifying Suspect or Illegitimate Products 13
Evaluation 1 13
Evaluation 2 14
Identifying Recalled Products 15
Evaluation 3 15
Evaluation 4 16
Speed and Accuracy of the Master Data Repository 16
Evaluation 5 16
Evaluation 6 17
Evaluation 7 17
Readability and Security of the RFID tag 17
Evaluation 8 17
Reliability, Accuracy, and Security of the MDR 18
Evaluation 9 - Security Risk Analysis 18
Evaluation 10 - Penetration Testing 19
Evaluation 11 - cGMP Audit on Centralized “Master Data” Repository 19
Accuracy with Disaggregation 20
Evaluation 12 20
Aggregation in Manufacturing 21
Evaluation 13 - Defect Rates 21
Evaluation 14 - Production Speeds 21
Evaluation 15 - Scalability & Costs 22

Part 3 - Implications for Supply Chain Participants 23
Suspect and Illegitimate Products 23
Implications for Manufacturer Aggregation 24
Implications for Wholesalers 24
Implications for Hospitals 24

Conclusions 25
DSCSA Is a Starting Point, Doesn’t Need Ubiquitous RFID 25
“Serialized Unit Doses” and a “Master Data Repository” is a Better Solution for Supply Chain Security 25
The Best Solution for Now: Saleable Unit Barcode + Unit Dose RFID 26

Introduction

Since 2012, Kit Check's medication intelligence platform has helped more than 500 hospitals track more than 100 million unit doses using a combination of two technologies: RFID tags with unique serial numbers and a cloud-based master data repository (MDR). Using these technologies, we've improved the state of hospital pharmacy by increasing efficiency, improving patient safety, and providing visibility into an important segment of the hospital's drug inventory. This has saved hospital pharmacy staff countless hours of manual inventory management and guesswork, virtually eliminated instances of expired and recalled medications from being restocked in trays and dispensing cabinets, and given pharmacy staff visibility into a large portion of their drug inventory which was previously untracked and poorly managed.

Our commercial work to date has focussed on unit-doses — primarily vials and syringes — because hospitals have recognized there's measurable value in implementing our technologies. In exchange for every $1 they invest in the solution, they get back more than $4 in cost savings and efficiencies, all while improving patient safety. This ROI is important to keep in mind because DSCSA, and any other program for that matter, can't reach its full potential if its not delivering net positive value to supply chain constituents and customers. In other words, we can't simply implement taxes and burdens, without also delivering value, and expect a program like DSCSA to reach its full potential. We know there has been tremendous investment in barcode-based technologies, and we believe they serve very important purposes. But we should be careful not to limit our thinking and our future success by enshrining the status quo without leaving room for, or even encouraging, innovation.

Although most of our work to date has been focused on unit-doses, the technology we've chosen — serialization coupled with an MDR — has broader applications and can easily be used to track drug products at other levels of aggregation such as the carton, case, and pallet. Since DSCSA has a focus on saleable units, most of this report will focus on use of the technology at that level, or discuss cases where it can be equivalently used at either the unit-dose or saleable unit level without much difference.

We know that DSCSA compliance will not be achieved by RFID alone, but our explorations throughout this pilot have convinced us that the combination of **barcode at the saleable unit coupled with RFID at the unit-dose, in many circumstances, presents a tremendous value proposition for numerous supply chain participants and customers, and allows us to better solve many of the problems that inspired DSCSA in the first place**. Not only will it help with existing manufacturer and hospital workflows, it is also a foundational technology that future tools and services can build upon to continue deliver more value to supply chain constituents and customers over time.

Most readers of this report will be familiar with barcodes and their use in the supply chain today. But for that same audience, RFID may conjure up memories of FDA mandates and commercial efforts (i.e. Walmart) which failed in recent decades. The reasons are myriad, including nascent RFID technology that was unreliable, cost burdens that were never offset by supply chain participants or customers getting true value from the technology downstream, and a world that didn’t yet have ubiquitous, fast, and reliable internet. That landscape looks very different in 2020, and our last 8 years in the marketplace has proven those days are largely behind us. To be clear, RFID is not the right solution for every problem, but the technology has changed tremendously since those early days and detractors would be well served to take a second look.

We appreciate the FDA’s decision to include us in the pilot process and their desire to foster a robust and forward-looking discussion. We believe the opportunity at hand is not only to improve supply chain security and follow the law, but to go further and consider our moral obligations to build an operate a supply chain that maximizes patient safety and makes smart use of attainable technologies to continue driving progress and improvement.

Part 1 - Technical Primers and Background

Before we get to our pilot evaluations and results in Part 2, we'd like to present a primer about the underlying technologies that we make use of throughout this pilot. We presume that most readers of this report are familiar with barcode technology's benefits and limitations, but we don't assume the reader has as much background on RFID and the use of modern cloud software architecture and master data repositories shared across hundreds or thousands of users. So while this section doesn't directly speak to the mandates of the pilot, we feel that it is an important foundation which will help the reader better understand our findings and our positions.

RFID Tags

Have you ever driven through a toll plaza and had your account automatically debited because of the transponder affixed to your windshield? Have you ever removed an item from your hotel minibar and been automatically charged (or overcharged, as is the case for many hotels!)? Have you noticed how certain clothing stores, such as Uniqlo, always have that shelf of jeans properly stocked with all sizes? All of these interactions are facilitated by RFID tags and readers.

The primary purpose of an RFID tag is to identify the object to which it's attached. In the examples above, those objects would be the toll pass account holder, the item you're removing from the refrigerator, and the pair of jeans on the shelf. The act of identifying these objects occurs when an RFID reader starts reading or scanning for tags in its vicinity. It does this by emitting radio waves (comparable to that of your cell phones) through its antennas. Any tags in its vicinity will pick up on those radio waves and respond back with some data; most commonly, that data is a unique serial number which can be used to identify the object upon lookup in a database. If there are multiple tags in the reader's range, they will all respond and the reader will collect a list of multiple serial numbers.

An "inlay" generally refers to the underlying RFID technology embedded within a tag or label. The inlay is typically a very thin substrate that combines an antenna and integrated circuit (IC). When a tag or label is being manufactured by a label converter, the inlay can be inserted into the label, typically between the top layer of paper or plastic and a lower layer of adhesive.

RFID tags and readers communicate using radio waves, and those waves can be influenced by their environment, affecting overall performance. For optimal performance, an RFID tag's antenna should be designed with particular use cases in mind. For example, we have worked with Avery Dennison to design a number of inlays to be used on unit-dose medications such as syringes and vials. The designs take into account the substrate to which the tag will be affixed, such as plastic or glass, as well as other elements in the environment, such as the liquid of a drug or the metal of its packaging. If not accounted for, each of these factors can act in subtle ways to interfere with, or detune, the radio waves, making the tag harder to read.

The cost of RFID tags has dropped precipitously over the last few decades and can be as low as a few pennies. In fact, cost is so low now that it’s largely just reflecting the underlying commodity prices such as silicon, copper, silver or aluminum. Because of the performance considerations described in the previous paragraph, it’s often worthwhile to spend an extra penny or two to get an inlay that performs reliably in the desired scenarios.

The inlay is controlled by its IC. This is similar to the Intel or AMD processor that controls your laptop, but with less processing power. Because it’s a digital chip, it can perform additional functions beyond storing and broadcasting a serial number (which we’ll make use of in a number of our pilot evaluations). For now, it’s sufficient to understand that the presence of an IC offers a number of authentication and encryption methods beyond barcode. This can allow for things like secrets, public/private keys, two factor authentication, etc.

Passive vs Active — As you explore the RFID landscape, you’ll find the term RFID applied to, and misapplied to, many variations of the core technology. Passive RFID refers to tags without a battery, such as those you would find in Kit Check or in your car’s toll pass. Active RFID refers to tags that have batteries and act as a beacon, broadcasting their serial numbers to any reader that is listening. These “active RFID” technologies often use other wireless protocols such as WiFi, Zigbee, etc. Everything in this report will be focussed on passive RFID.

LF, HF, and UHF — Passive tags are further subdivided into a few categories: low frequency (LF), high frequency (HF), and ultrahigh frequency (UHF). These names correlate to frequency ranges on the electromagnetic spectrum in which they receive and respond. Different frequencies will perform better or worse in different environments. Many people reading this report have probably heard of NFC; that uses a particular type of HF.

EPC, TID, and Extended Memory — EPC and TID are fields, or memory banks, on the tag which are used to store numbers. EPC is short for electronic product code, but will often times be referred to as the tag’s “serial number.” The EPC can be changed by users and locked with passwords. The TID is a similar serial number that can only be written by the IC manufacturer and never altered by users. Some older inlays also have extended memory for storing additional data, but these older chips have worse RF sensitivity and have largely fallen out of favor.

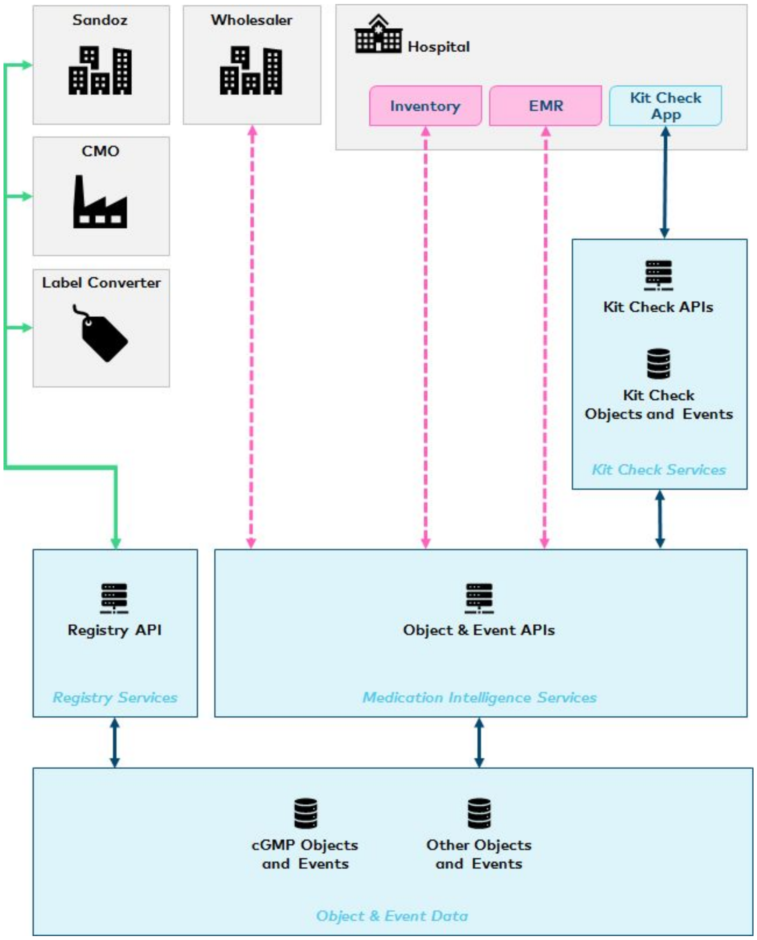
UHF Class 1 Gen 2 — This is the standard that most modern UHF tags and compatible readers follow. There is also an industry consortium called RAIN which has applied its namesake as a branding of UHF Class 1 Gen 2 in much the same way that Wi-Fi is a branding for multiple parts of the IEEE 802 protocol family.

Throughout this document, we’ll be talking about UHF Class 1 Gen 2 tags and will simply refer to them as RFID tags or inlays. In general, they have proven to be the most useful for tracking and inventory purposes in the pharmacy to date, though there may be scenario-specific exceptions to this rule.

Master Data Repository

Modern Cloud-based Software Architecture

The Bluesight platform (on which Kit Check is built) is comprised of multiple cloud-based applications and services. It acts as the master data repository (MDR) and provides end-to-end medication intelligence services that can be easily integrated with other technologies throughout the drug supply chain.



In 2011, when we started building this, we chose to follow the lead of other modern, successful platforms like Gmail and Salesforce because of the many advantages that cloud computing platforms offer. This approach has become commonplace in the years since and, more recently, we've seen many within the industry starting to understand and appreciate these benefits.

With a centralized cloud offering, companies and users don't have to maintain servers, upgrade software, perform backups, or be responsible for implementing cutting edge security. Additionally, if properly architected, cloud services can easily scale to support very large datasets and computing needs.

Single Source of Truth

Most importantly, as it relates to DSCSA, the MDR can be a single source of truth into which many supply chain participants can integrate, providing a centralized view and near real time tracking of saleable units (or even unit dose medications) from manufacturers to hospitals.

This centralized approach is crucial to unifying and exposing relevant data to authorized parties about each item in the supply chain. To illustrate why this centralized approach is important, consider a refrigerated medication such as rocuronium. When the manufacturer produces a vial of it, they will associate a standard expiration date to that vial and print it on the label. Eventually, that vial gets stored in a hospital's refrigerator and later removed, causing the need to calculate and store a beyond use date (BUD). Today, most sites will write that date on a sticker and place it on the vial. But if that vial is then used in a dose prep system, a dispensing system, or a syringe labeling system — even if those systems can read the original expiration date off a barcode — those systems have no idea what the BUD is.

Contrast this to a system where you make use of the rocuronium vial's serial number and a central repository. In that system, the following can happen in an easily coordinated fashion:

1. The manufacturer stores the "number of days" needed for a beyond use calculation for that NDC, for example "30 days."
2. The CMO stores the expiration date during manufacturing activities.
3. The connected refrigerator creates a "removed from refrigeration" event.
4. The centralized platform calculates the "beyond use date" based on data from #1-3 and rules for that NDC.
5. The downstream system (such as a dose prep, dispensing, or syringe labeling system) looks up that serialized item and gets the earlier of the expiration date (from step #2) and the beyond use date (from step #4).

Without a centralized approach, you're relegated to storing data on the item's RFID tag or syncing serial numbers and expiration dates between multiple systems managed by multiple parties. Each of these approaches has drawbacks such as needing to maintain redundant data stores, problems with syncing data, lack of clarity around the data's source of truth, and challenges with detecting and preventing data corruption and counterfeiting attempts. Legacy systems, such as EPCIS, exhibit various forms of these problems once you start to consider multiple trading partners handling inventory from multiple manufacturers and shipping to multiple customers.

In 2020, we expect to track double the number of serialized items as we've tracked in our company's entire history. Using several standard and efficient cloud computing techniques, we can effortlessly expand our platform to accommodate that growth and much more. In part, this growth can be facilitated by larger databases and computing capacity. But as important, it also includes logical and geographic redundancies so the system can remain resilient when the unexpected happens. For example, if a major earthquake took out our primary East Coast data center, we employ real time replication to keep up-to-date backups of that data in data centers around the country, along with redundant applications and services which can be fired up instantaneously based on traffic patterns and other triggers. From the user's perspective, the earthquake was a non-event and their usage of the system can continue uninterrupted.

cGMP in the Cloud

In 2019, as our relationships and partnerships with pharma manufacturers matured, we upgraded our applicable software and services to fit with their cGMP requirements. Our *Registry Service*, for example, was designed with two major cGMP-related principles in mind. First, our internal processes for creating requirements, building software, quality assurance testing, deploying upgrades, maintaining a production environment, and offering ongoing service and support, have changed to follow cGMP processes and principles. Second, we recognize that cGMP facilities will now be integrating with our software, so it must easily fit into their world of control, qualification, and validation.

For our platform to truly succeed and deliver value to all its users, integration with technology throughout the supply chain is important. Even with our first medication management workflow tool, Kit Check, we designed it so that the front-end workflow tool was separate from the back-end platform services. This kind of architectural separation is common place in platform development and allows the system to be more modular, scalable, and supportable. But as important, it facilitates integration with other systems. For example, the hypothetical dose prep, dispensing, and syringe labeling systems that we mentioned above could easily connect through our web-based APIs — that's *application programming interfaces*, not *active pharmaceutical ingredients* — quickly and easily with minimal upfront costs.

System Security, Reliability, and Accuracy

With any mission critical system, security plays a crucial role and a platform centered on drug supply chain data is no exception. Luckily, it's 2020 and the world is starting to get its act together when it comes to security. We have the tools — encryption, two factor authentication, no- and low-trust environments, etc. — to build these platforms the right way, and it's incumbent upon all of us to take responsibility for doing so. Gone are the days when technical security and system integrity could be an afterthought.

Kit Check takes security very seriously and, in Evaluations 9, 10, and 11, we outlined a number of third party audits that speak to the architectural, physical, logical, and procedural security mechanisms we've implemented over the years for our systems and data, and additional safeguards for subsystems related to HIPPA- and cGMP-relevant data. Because of this focus, and commensurate resources we've allocated, we're able to consider security of the MDR and enforce best practices throughout our partner ecosystem rather relying on a spotty patchwork of home-grown efforts from each individual participant.

Barcodes vs RFID Tags

When thinking about DSCSA requirements and the supply chain, many people default to thinking about barcodes and quickly write off RFID technology as being too expensive. In some respects, this is an understandable behavior. Whether due to past RFID projects that failed due to cost or technical limitations, succumbing to the sunk cost fallacy relative to current barcode-driven infrastructures, or because of recency and primacy effects related to "everyday barcode exposure," it's clear that barcodes get the benefit of the doubt in cases where RFID might actually be superior.

As part of this primer, we felt it was valuable to highlight some of the differences between RFID and barcodes, and when each might be most appropriately used. When evaluating the use of barcode vs. RFID as a data carrier, there are a number of important factors to consider. Below is an exploration of some of the more important factors, including pros and cons of each. While this list is not exhaustive, a consideration of these factors will go a long way in helping to choose the best option for any particular project or challenge.

Line of Sight — In order to scan a barcode, there must be a line of sight between the scanner and the barcode. This means the object containing the barcode must be positioned and oriented so the barcode is visible to the scanner and there is nothing between the object and scanner to obstruct its view. These constraints become important in a few scenarios.

- Aggregation, especially in the case of packaging cartons into cases, is probably the most common. Typically, the aggregation causes some or all of the inner items' barcodes to be obstructed from an outside scanner.
- Conveyance is extremely common in the supply chain, from wholesaler totes to hospital kits and trays. These ad hoc groupings are useful for the transportation and management of medications, but quickly inventorying the contents of these containers and groupings is much better achieved using RFID.
- Dense storage setups, such as warehouse shelves, pharmacy carousels, and pharmacy box-pickers, represent other temporal forms of aggregation and pose a challenge to quickly inventorying contents when line of sight is needed.

Read Speed: One vs. Many — In many workflows, there is a need to collect information from a plurality of items. Using barcode, each item must be oriented and scanned individually. Using RFID, hundreds or thousands of items can be scanned simultaneously. Depending on the nature and constraints of the workflow, RFID can be orders of magnitude faster than barcode.

Read Range: Feet vs. Inches — Most barcode scenarios work best when there is a short distance between the scanner and the barcode. This is dependent on both the scanner quality and the barcode's size, resolution, print quality, and materials. In the case of RFID tags and scanners, the read range can easily be dozens of feet (depending on environmental and technical factors).

Interference & Durability — RFID tags and barcodes are both physical objects subject to wear and tear which can affect read performance. For barcodes, visual quality can be degraded when labels get dirty, experience wear and tear from environmental factors, or get torn, removed, or otherwise damaged. For RFID tags, their ability to function well can be affected by environmental factors such as proximity to certain solid and liquid materials, elements acting as Faraday cages or blocking signals, and radio interference.

Data Integrity — Data integrity is important for basic functionality ("Can I read this carrier's data?") and for enabling more sophisticated and specialized requirements such as authenticity ("Do I know this label hasn't been cloned or counterfeited?").

Barcodes can incorporate a variety of techniques such as check digits and hashes to help assure the integrity of the data, though these are limited by the relatively small dataspace of the barcode and its analog nature.

RFID tags have a number of technical mechanisms to increase assurances of data integrity:

- Checksums are built in to read and write protocols

- The TID is an immutable and unique number that can be used to detect counterfeiting attempts
- Data can be locked to ensure it hasn't been tampered with
- Tags can be killed in the even that it's determined valuable

Cost: Unit Cost vs. Total Cost of Ownership — When using a data carrier technology in inventory, aggregation, authenticity, and recall management scenarios, the requirements don't usually stop with the mere presence of an identifier. There are workflows — manual or automated, systematized or ad hoc — associated with all of these scenarios, and those workflows cost money. So it's important to consider if the presence of a barcode or RFID tag makes the overall workflow and solution cheaper or more expensive.

In many scenarios, the discrete act of getting a barcode on a product will be cheaper than getting an RFID tag on that same product. But it's also important to consider the "total cost of ownership" of that product throughout the supply chain. Factoring in things like human beings scanning millions of barcodes one by one, instead of RFID readers working in large aggregates, the difference in "total cost" can begin to diverge quickly. If we look at the tags that are used by hospitals for kit and tray management today, there's about $4 in savings for every $1 of RFID-related cost for the hospital. This savings comes from the hospital's ability to leverage the presence of the RFID tag to reduce inventory management labor, reduce expired drug waste, improve recall handling, and other reductions in other inefficiencies.

Usability — Because of a number of factors already listed here, the human experience of working with these technologies can vary widely. With barcode, you have people scanning many items; for example, scanning cartons during aggregation or scanning unit doses in inventory replenishment workflows. These are repetitive, tedious, and time consuming tasks, all of which can lead to errors, injury, and other undesirable outcomes. In surveys and discussions, many workers find the efficiency, convenience, accuracy, and ergonomics of RFID-based workflows to be significantly better than their barcode equivalents.

Blockchains

In 2020, we'd be remiss not to mention blockchain, a distributed and immutable leger with elements of scarcity and trust built in at the protocol level. It is a revolutionary and important technology. Arguably, it's the most important protocol to come along since the the collection of protocols that enable email and the web (TCP, IP, SMTP, POP, IMAP, HTTP/S, etc.).

As technologists, we're often drawn to new technologies and get excited about exploring their possibilities, but it's important to evaluate these against the problem we're trying to solve, and honestly weigh the costs and benefits without getting carried away by "shiny object syndrome." In the case of tracking items through the supply chain, we think the benefits and reduced costs of a trusted MDR far outweigh the costs of blockchain. Immutability is not really the right tool when proper role-based security and trusted intermediaries are so readily available. And in an industry such as healthcare, where technology routinely lags years behind the state of the art, trying to get meaningful adoption of a distributed system will prove to be nearly impossible in any reasonable timeframe.

Additionally, blockchain has other esoteric weaknesses such as 51% attacks, slow settlement, ledger size growth, inefficient computing resources, etc., that we won't cover here. But be aware that although vendors will tell you that their *proprietary* blockchain solutions overcome these weaknesses, they often fail to mention that, in their attempts to overcome these, they're essentially recreating the trusted centralized solutions that they're claiming to have advanced beyond.

Part 2 - Pilot Evaluations and Findings

This section describes our pilot evaluations and results.

Identifying Suspect or Illegitimate Products

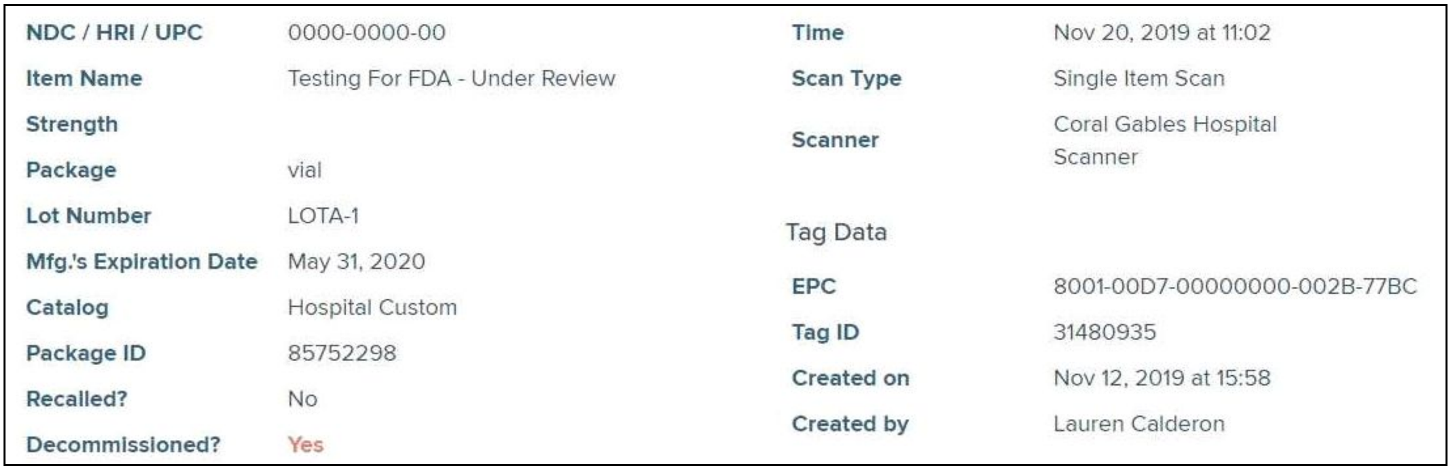
In this set of evaluations, we set out to test the ability of the MDR to assist in identifying suspect or illegitimate product. We evaluated this in two different ways to illustrate a variety of responses that could be hospital- or manufacturer-lead.

Evaluation 1

In this evaluation, we simulated a scenario where the manufacturer has already shipped an item and then discovered that it is suspect before the hospital received it. Our evaluation followed this process:

- Tag the item and register it in the MDR
- Ship the item to the hospital
- Determine/discover that the item is suspect or illegitimate
- Mark the item unusable in the MDR
- Hospital receives the shipment and attempts to scan the item into inventory
- The scan results inform the pharmacy staff member that the item is unusable

The MDR allows the manufacturer to blacklist the item so that, when the hospital receives and scans that item into their inventory, the system will inform the pharmacy staff member that this item shouldn't be used. It also renders that item unusable in downstream systems which lookup the suspect drug.



NDC / HRI / UPC	0000-0000-00
Item Name	Testing For FDA - Under Review
Strength	
Package	vial
Lot Number	LOTA-1
Mfg.'s Expiration Date	May 31, 2020
Catalog	Hospital Custom
Package ID	85752298
Recalled?	No
Decommissioned?	Yes

Time	Nov 20, 2019 at 11:02
Scan Type	Single Item Scan
Scanner	Coral Gables Hospital Scanner

Tag Data

EPC	8001-00D7-00000000-002B-77BC
Tag ID	31480935
Created on	Nov 12, 2019 at 15:58
Created by	Lauren Calderon

In this evaluation, we uniquely targeted the suspect item by its EPC (the unique serial number assigned to that item, encoded to its RFID tag, and registered in the MDR). If more than one item was suspected, we could target a list of many EPCs.

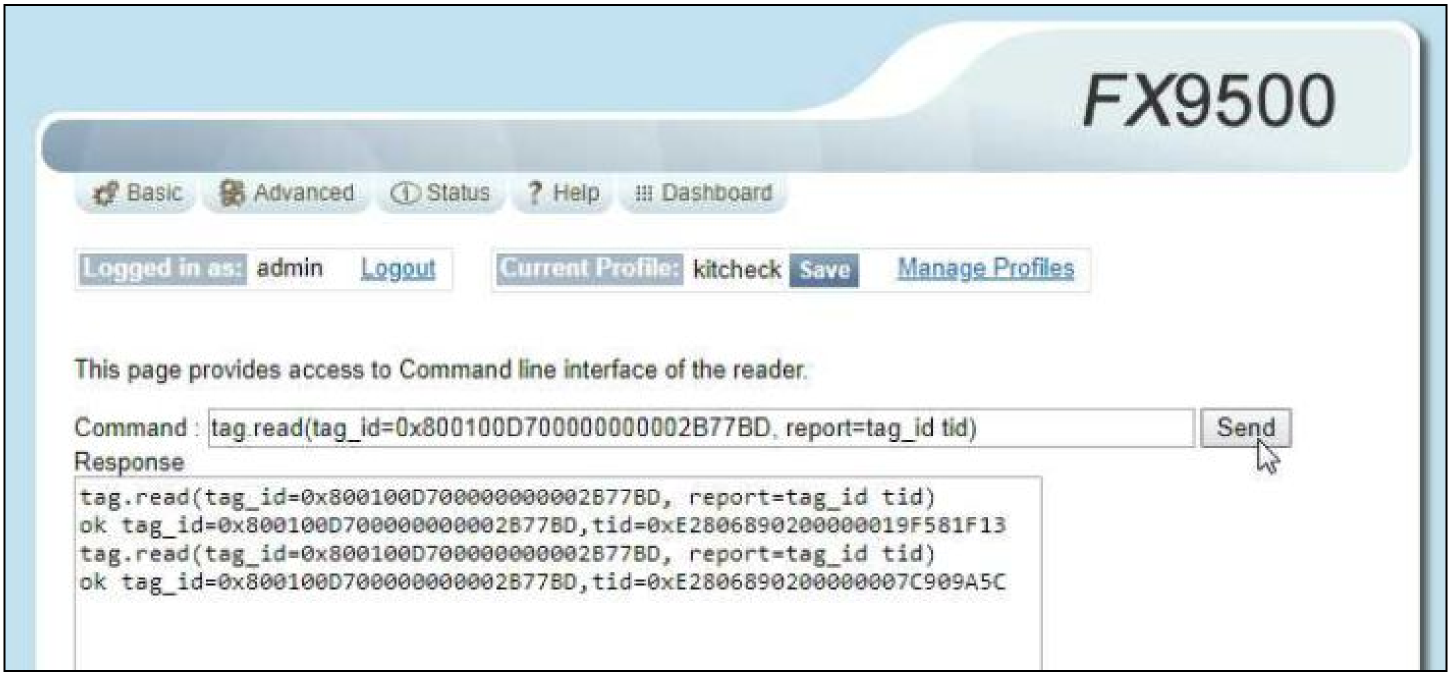
Beyond individual items and lists of many EPCs, we can also target items by other attributes such as NDC and Lot Number. Similar to our evaluations of recall handing (see below), if we believed an entire lot to be suspect, we could blacklist all the items in that lot.

Finally, we can track reasons for why an item is blacklisted and display those to the user or use them in reporting and analysis. Examples of such reasons might be generic (i.e. suspect or illegitimate product) or specific (i.e. ingredient X in lot Y was determined to be counterfeit).

Evaluation 2

In this evaluation, we simulated a counterfeit tag/label to test if we could automatically determine that the product should be considered suspect. Our evaluation followed this process:

- Tag the real item ("REAL") and register it in the MDR
- Attempt to counterfeit the label and tag from REAL by creating a new fake label ("FAKE") and encoding REAL's EPC on FAKE's tag
- Ship FAKE to the hospital
- Hospital receives the shipment and attempts to scan the FAKE item into inventory
- We look up FAKE's EPC and TID in the MDR, determine that the TID doesn't match, and automatically declare the item to be suspect or illegitimate



Logged in as: admin

Current Profile: kitcheck

This page provides access to Command line interface of the reader.

Command : tag.read(tag_id=0x800100D700000000002B77BD, report=tag_id tid)

Response

```
tag.read(tag_id=0x800100D700000000002B77BD, report=tag_id tid)
ok tag_id=0x800100D700000000002B77BD,tid=0xE2806890200000019F581F13
tag.read(tag_id=0x800100D700000000002B77BD, report=tag_id tid)
ok tag_id=0x800100D700000000002B77BD,tid=0xE2806890200000007C909A5C
```

In Evaluation 1, we relied on the manufacturer explicitly declaring an item to be suspect. In this evaluation, we're using unalterable attributes about the REAL item to verify alleged instances of that item further downstream in the supply chain. Specifically, in this case, we're comparing the REAL's unalterable TID registered during manufacturing to that of the item which arrived at the hospital, FAKE, and we can easily determine that the EPC/TID pair in the MRD doesn't match the EPC/TID of the FAKE item that arrived at the hospital.

NOTE: For a more in depth discussion of EPC/TID pairs, please see our writeup on Suspect and Illegitimate Products in Part 3 of this report.

Identifying Recalled Products

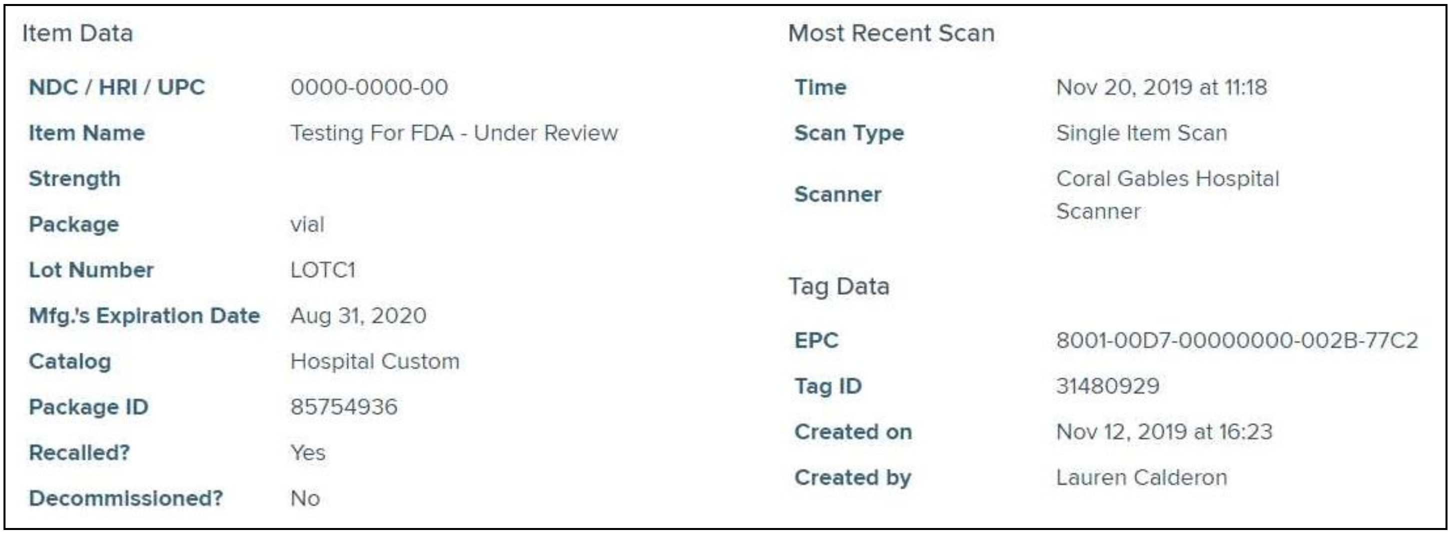
In this set of evaluations, we set out to test the ability of the "master data" centralized repository (MDR) to assist in handling recalled product once its been distributed throughout the supply chain. Similar to Topic 2, we evaluated this in three different ways to illustrate a variety of responses that can be hospital- or manufacturer-lead and proactive or reactive.

Evaluation 3

In this evaluation, we simulated a scenario where the manufacturer has already shipped an item and then recalls it before the hospital receives it. Our evaluation followed this process:

- Tag the item and register it in the MDR
- Ship the item to the hospital
- Issue a recall for the item
- Register the recall in the MDR
- Hospital receives the shipment and attempts to scan the item into inventory
- The scan results warned the pharmacy staff member that the item is unusable because it has been recalled

The MDR allows the manufacturer to register a recall so that, when the hospital receives and scans that item into their inventory, the system will alert the pharmacy staff member that this item shouldn't be used because it has been recalled. It also renders that item unusable in downstream systems which lookup the recalled drug.



Item Data

NDC / HRI / UPC	0000-0000-00
Item Name	Testing For FDA - Under Review
Strength	
Package	vial
Lot Number	LOTC1
Mfg.'s Expiration Date	Aug 31, 2020
Catalog	Hospital Custom
Package ID	85754936
Recalled?	Yes
Decommissioned?	No

Most Recent Scan

Time	Nov 20, 2019 at 11:18
Scan Type	Single Item Scan
Scanner	Coral Gables Hospital Scanner

Tag Data

EPC	8001-00D7-00000000-002B-77C2
Tag ID	31480929
Created on	Nov 12, 2019 at 16:23
Created by	Lauren Calderon

NOTE: A variation of this method is used in hospitals around the country today for unit-dose medications stocked in kits and trays (i.e. an emergency med tray in the top drawer of a crash cart, an anesthesia tray in the OR, etc.). These systems, including Kit Check, track the lot number of each tagged vial or syringe and know in which tray each vial or syringe is stocked. When a recall is registered, the system can tell pharmacy staff where to go to retrieve recalled items and prevent those items from being restocked into kits and trays in the future.

Evaluation 4

In this evaluation, we explore a slight variation on Evaluation 3 where the recall doesn't get registered in the MDR until after the hospital has received and started using the item. By searching the MDR, we were able to determine that the hospital had already received our "test item" into inventory and that it matched the recall criteria. From there, we were easily able to provide instructions for the hospital on where to find it for easy removal.

In practice this evaluation goes beyond DSCSA and would require the MDR to maintain some link between the saleable unit (against which the recall is entered) and the serialized vials with it. This is trivial if the hospital employs a system like Kit Check and it's a great example of why you may want a hybrid world where the saleable unit's serial number is in a barcode, the unit dose's serial number is in an RFID tag, and the two are linked together in the MDR.

Speed and Accuracy of the Master Data Repository

In this set of evaluations, we set out to test the speed and accuracy of the MDR.

Evaluation 5

This evaluation looks at the speed of registering new items, in bulk, in the MDR. This evaluation was designed to mimic what a manufacturer or CMO would experience when registering the contents of their production batches. The following timings were observed:

Number of items registered at once	Time to complete registration
10,000 items	1.4 seconds
100,000 items	14.4 seconds
500,000 items	94.9 seconds

From the manufacturer's perspective, these results are exceedingly acceptable given the batch-oriented nature of their workflows and operations. From a technical perspective, it would be relatively easy to dramatically speed up these times if the workflow necessitated it.

Evaluation 6

In This evaluation, we had one user create and encode 100 RFID tags. The user entered the NDC, Lot Number, and Expiration Date into the system and let it generate 100 unique EPCs. These EPCs, and related data, were registered in the master data repository and the physical tags were encoded using an RFID printer. Then, a second user, took those 100 tags and attempted to read back the the tags' data (EPCs, NDC, Lot Number, and Expiration Date) and verify that it was accurate. They used Kit Check's *Verification* workflow feature to perform the check. The results showed that 100% of the tags got encoded with the correct EPCs and 100% of the data registered in the master data repository was returned and verified to be accurate.

Evaluation 7

This evaluation looks at the ability to read items on the manufacturing line and the related effects on line speed and accuracy. Kit Check has built hardware that manufacturers and CMOs can install on their lines to read serial numbers and other item data from packaging barcodes, and register that data in the MDR. So far, we've tested up to 750 item tags and 30 carton barcodes per minute on a conveyor moving at 60 feet/min and are reading 100% of the items accurately. We don't yet know the upper bounds of this speed (while maintaining 100% accuracy), but we're already well in the realm of speeds that you'll find on typical vial manufacturing lines and believe we can increase this throughput if necessary.

Readability and Security of the RFID tag

Evaluation 8

In this evaluation, we took a number of Kit Check's *Basic Tags* and tried to change their pre-encoded EPCs. The Basic Tags have unique EPCs encoded on them during manufacturing and are "locked" using the UHF Gen2 native locking functions and access passwords. The results showed we were unable to change the EPC. We further attempted to unlock the tag using the default "all zeros" password and other randomly guessed passwords, and were still unable to unlock it.

This evaluation showed that, when proper techniques and workflow steps are used, data on the tag is accurate and can be relied upon to read back as the manufacturer or encoder intended.

Reliability, Accuracy, and Security of the MDR

Kit Check has built its systems with security in mind from day one. We realized early on that a centralized medication intelligence platform would provide immense value to all participants in the supply chain, but in order to see the value materialize, it is critical that our systems are built and maintained in a secure, robust, and trusted way. Item attributes and events are at the core of that system and Kit Check spends significant resources ensuring the reliability, authenticity, integrity, and usability of that data.

One critical component of delivering on that promise is security. Since its inception, Kit Check designed and built our system with security in mind. Doing this in the cloud in 2011 was not always easy or encouraged, but as technology has evolved and supply chain participants — particularly hospitals — have become more sophisticated and more reliant on our services, this has proved to be one of the crucial foundations of our offering.

Kit Check's technology is frequently audited by hospital customers, pharmaceutical manufacturers, and other partners. Recently we've had three large, reputable third parties perform independent security assessments of our cloud platform and process/risk assessments of our operations. We'll summarize those results here to show that a centralized MDR can be built and maintained in a secure manner and trusted by users throughout the supply chain.

NOTE: For security purpose, and to respect confidentiality agreements, we can't disclose certain details about these evaluations; however, we promise to faithfully represent the spirit of those accounts here and can make available such reports to business partners at appropriate stages of those partnership relationships.

Evaluation 9 - Security Risk Analysis

The first assessment was a **Security Risk Analysis** which aimed to identify threats, vulnerabilities, control gaps, and weaknesses which presented risk to Kit Check systems and data. The assessment concluded that, "Overall...compliance is adhered well, with Kit Check, Inc. appearing to have a mature security program."

The assessment elaborated:

> "Kit Check has a very mature and strong security posture with well-developed policies and procedures along with advanced technical safeguards implemented. Kit Check has the backing of senior level executive management to ensure that security is a priority throughout the entire organization. Some areas of strength for Kit Check, Inc. are as follows:
>
> "1. Policies and procedures regarding Kit Check Inc.'s information security program are robust and descriptive.

> “2. Technical implementation of the security controls is well-documented and supporting artifacts adhere to the requirements.”

As any security expert knows, good security hygiene includes an ongoing practice of risk assessment and mitigation. The report concludes by reinforcing that idea and suggesting that Kit Check’s future opportunity is in performing risk analysis regularly, and as the environment changes, which we have committed to doing.

Evaluation 10 - Penetration Testing

Another significant evaluation recently completed was **Penetration Testing**, sometimes known as a “pen test” or “ethical hacking.” This was run by a large reputable partner who selected their own large reputable third party to perform the tests. Kit Check had no influence in the decision of who performed the testing.

The objective of their testing was to “assess the effectiveness of the technical security controls implemented within the application and its supporting infrastructure.” The testing employed a methodology designed to “identify and exploit security vulnerabilities and misconfigurations.”

The scoring methodology used by this testing vendor is the Common Vulnerability Scoring System, Version 3. The report found no Critical, High, or Medium vulnerabilities, and the partner was extremely satisfied with how the results and conclusions reflected upon us, our systems, and our processes and procedures.

Evaluation 11 - cGMP Audit on Centralized “Master Data” Repository

Now that pharma companies are embracing our solution for unit-dose medication intelligence, some of them are contemplating ways to incorporate it into their cGMP facilities and processes and/or use it in conjunction with cGMP-relevant drug data.

Although cGMP is a relatively new discipline for us, we have embraced these manufacturers’ requests for a number of reasons.

- If we are to truly maximize the value that our platform can deliver to supply chain participants, we must offer solutions that can integrate seamlessly with their products and operations.
    - For manufacturers, this means qualified and validateable equipment and software that can enable RFID on their lines.
    - For mid- and down-stream supply chain participants, this means providing assurances around cGMP-relevant data that can be incorporated into workflow tools and decision-making processes (for example, recall handling).
- Most manufacturers are not experts at RFID or developing software platforms that scale. They want a best-of-breed solution that can be quickly installed on/near their lines and easily validated.

- Hospitals want a product that “just works.” This approach allows us to ensure uniformity and high quality levels across multiple vendors.

We recently facilitated a major pharmaceutical company’s **cGMP audit of Kit Check**. The audit covered “the activities and systems involved in the validation, testing, release and overall management and control of the data stored within the [MDR] software owned and operated by Kit Check. This includes both the back-end registry software and front-end interface used by [customer’s name omitted].”

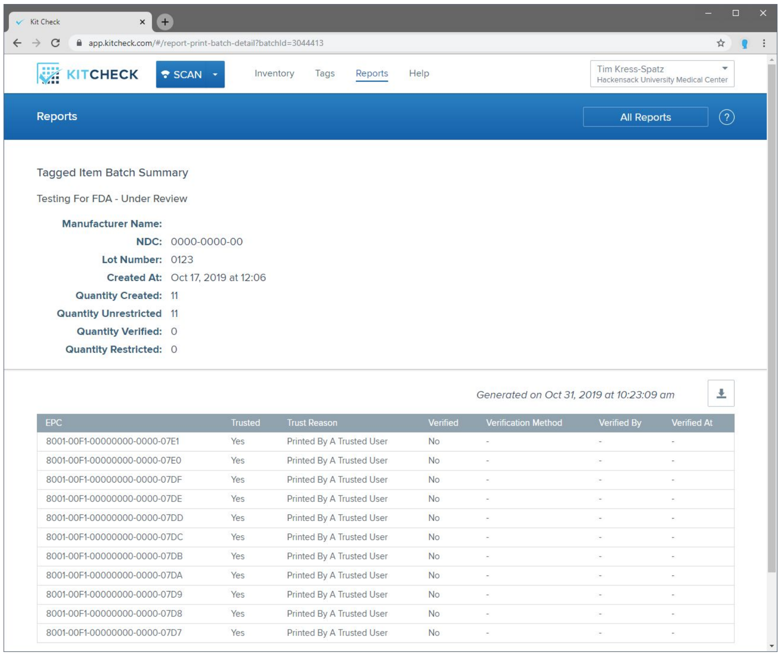
They findings summary stated, “Based on the observations and the reasoning denoted here, the outcome of the audit was determined to be Satisfactory.” The audit did convey a few observations and resulted in a small number of CAPAs, all of which were quickly remedied by October, 2019. As a relative newcomer to the world of cGMP, we were extremely proud of these results and look forward to assisting more manufacturers in the future.

Accuracy with Disaggregation

Evaluation 12

This evaluation simulated the disaggregation of bulk product (i.e. a case which contains multiple cartons) in an effort to test our ability to track the lower-level packages (i.e. saleable unit “cartons”). The goal was to evaluate the following questions:

1. Given the original aggregate batches (case), could we track the constituent items (cartons) after disaggregation and as they flowed through the supply chain to the hospital?
2. Given a single disaggregated item (carton) at the hospital, could we track it back to its original aggregate batch (case)?


Kit Check
app.kitcheck.com/#/report-print-batch-detail?batchId=3044413
KITCHECK
SCAN
Inventory
Tags
Reports
Help
Tim Kress-Spatz
Hackensack University Medical Center
Reports
All Reports
?

Tagged Item Batch Summary

Testing For FDA - Under Review

Manufacturer Name:
NDC: 0000-0000-00
Lot Number: 0123
Created At: Oct 17, 2019 at 12:06
Quantity Created: 11
Quantity Unrestricted 11
Quantity Verified: 0
Quantity Restricted: 0

Generated on Oct 31, 2019 at 10:23:09 am

EPC	Trusted	Trust Reason	Verified	Verification Method	Verified By	Verified At
8001-00F1-00000000-0000-07E1	Yes	Printed By A Trusted User	No	-	-	-
8001-00F1-00000000-0000-07E0	Yes	Printed By A Trusted User	No	-	-	-
8001-00F1-00000000-0000-07DF	Yes	Printed By A Trusted User	No	-	-	-
8001-00F1-00000000-0000-07DE	Yes	Printed By A Trusted User	No	-	-	-
8001-00F1-00000000-0000-07DD	Yes	Printed By A Trusted User	No	-	-	-
8001-00F1-00000000-0000-07DC	Yes	Printed By A Trusted User	No	-	-	-
8001-00F1-00000000-0000-07DB	Yes	Printed By A Trusted User	No	-	-	-
8001-00F1-00000000-0000-07DA	Yes	Printed By A Trusted User	No	-	-	-
8001-00F1-00000000-0000-07D9	Yes	Printed By A Trusted User	No	-	-	-
8001-00F1-00000000-0000-07D8	Yes	Printed By A Trusted User	No	-	-	-
8001-00F1-00000000-0000-07D7	Yes	Printed By A Trusted User	No	-	-	-

To prepare for the test and attempt to create the requisite data trail, we tagged a number of constituent items (simulated cartons) comprising the contents of two aggregate batches (simulated cases). We then disaggregated those batches into their constituent items, split them in half, and shipped them to our two partner hospitals — Hackensack University Medical Center and Coral Gables Hospital — who scanned them upon receipt.

To perform the actual test, we first looked up the original case and its constituent cartons. We then looked up all 21 of those cartons and could see an accurate trail of their creation and eventual receipt by the two hospitals. Second, we attempted to work backwards (as a hospital might want to do up on receipt), by looking up some of the cartons, and we could accurately see the original cases from which they were disaggregated.

The evaluation confirmed that, even after disaggregation, individual and batch elements had been tracked properly and disaggregation, and subsequent receipt by multiple parties, didn’t adversely affect the tracking in any way.

Aggregation in Manufacturing

In manufacturing facilities, Kit Check and Sandoz (a division of Novartis) have assessed the error rate in manual and automated processes on packaging lines. Specifically, we are comparing barcode- and RFID-based approaches to aggregation. We know that current workflows, where a human scans DSCSA-mandated serialized barcodes on cartons and cases during aggregation, are error prone. These errors lead to bad data in tracking systems and inaccurate transmissions between trade partners. In our testing of an RFID-based workflow — aggregating first and then RFID-scanning the constituent parts in aggregate — we are seeing zero errors.

Evaluation 13 - Defect Rates

Barcode rejection rates are less than 1%, primarily caused by printing errors manifesting in packing stations. By comparison, our early tests of RFID show that 1 out of 2,000 RFID tags didn't read properly, a much lower error rate of just 0.05%.

Although this already represents an improvement of more than one order of magnitude, the use of this RFID technology in cGMP manufacturing facilities is still new. We believe the error rates for RFID can be significantly lower with additional time to improve and tune the technology.

Evaluation 14 - Production Speeds

In this evaluation, we compared barcode based aggregation workflows to RFID based ones. The introduction of RFID Equipment had no effect on line speeds of 400 units per minute. Our tests of the RFID tunnel show that we can read the items’ RFID tags at full speed (along with their printed barcode for additional association workflows).

In terms of OEE (overall equipment effectiveness), the following have been observed:

1. Introduction of barcode-based serialization caused a 1-2% drop of OEE
2. Introduction of barcode-based aggregation caused a drop of OEE of
    a. 4-6% for manual pack out
    b. 2-4% for automatic case packers
3. Adding RFID serialization on the pack line showed no drop in OEE

4. Using barcode-based serialization and RFID-based aggregation reduces the effect on the pack line to 1-2% (this is essentially a combination of #1 and #3)

Issues number 1 and 2 (above) were caused primarily because barcode-based systems tend to have problems relating to the alignment of readers to barcodes.

Evaluation 15 - Scalability & Costs

In this evaluation, we compared the cost of equipment and labor for barcode based aggregation workflows to RFID based ones.

Approximate costs for purchasing and installing equipment to support each of the following scenarios:

1. Barcode-based serialization = $250,000
2. RFID-based serialization = $60,000
3. Barcode-based serialization + barcode-based aggregation = $400,000 to $600,0000
4. Barcode-based serialization + RFID-based aggregation = $310,000

(Scenario #4 is essentially a combination of #1 and a variation of #2. You can use the hardware in #2 for serialization, aggregation, or both, but the cost doesn't really change.)

Taken together, the cost of equipment for Scenario #3 is significantly more expensive than the cost of equipment for Scenario #4.

There are some additional costs which should be considered. 2D barcode printing adds 3-4 cents, and this would apply in both Scenarios #3 and #4. In Scenario #4, there are some additional costs and savings:

- Upgrading to RFID labels (insertion, encoding, and QA) will add 6-8 cents
- Manual packaging labor can be reduced by 1-3 people (depending on line speed) when using RFID-based aggregation
- The elimination of aggregation errors, when using RFID-based aggregation, can also lead to better compliance of data integrity requirements

Part 3 - Implications for Supply Chain Participants

Suspect and Illegitimate Products

DSCSA requires trading partners to identify suspect products. In part, suspect product is defined as a product for which there is reason to believe it is potentially counterfeit, diverted, or stolen. An RFID tag — particularly one embedded into a manufacturer's official packaging and labeling — contains a number of technical elements enabling it to be a useful tool in making such determinations about suspect products.

One of the simplest foundational technologies in an RFID tag is the manufacturer's tag identification (TID) number, a unique and immutable number encoded in the tag's TID memory bank. All standard UHF Class 1 Gen 2 RFID tags have this. The spec ensures that no two tags will have the same TID number and that, once encoded, the number cannot be changed.

When manufactures produce and tag items, they can collect EPC/TID pairs from each of those items and register them — along with other item attributes such as NDC and Lot Number — in the MDR. Later, at key checkpoints downstream in the supply chain, trading partners and end users with physical access to items can scan and lookup those items to validate the EPC/TID pairs against that which was originally registered in the repository by the manufacturer. Because TID is universally unique and immutable, it would be virtually impossible to create a second tag bearing the same TID for use on a counterfeit product or in a replacement/decoy product designed to disguise diversion or theft.

Despite our use of the word "impossible" in the previous paragraph, we recognize that many things aren't truly impossible, just expensive, inefficient, infeasible, or downright ridiculous. Given enough resources, many techniques and technologies can be circumvented. In this case, if you were a counterfeiter wanting to write your own TID on a tag, you'd effectively need control of an IC fab (an expensive manufacturing facility where you can fabricate your own integrated circuits) in order to encode numbers in your tags' TID memory banks. This is a very, very expensive proposition.

If the expense and impracticality of controlling an IC fab weren't enough, the second aspect of this technique — EPC/TID registration in a trusted, centralized repository with downstream lookups — dramatically increases the effectiveness of using TID for detection. A would-be counterfeiter would have to pilfer the number of units they want to counterfeit and repurpose those tags. But a pattern of strange downstream lookups would begin to emerge quickly; in other words, you couldn't create very many counterfeit units without being caught.

Finally, to further increase security, the item's TID should not be shared publicly. The manufacturer, MDR, and any other party or system with access to such data should only answer yes/no questions about the matching status of an EPC to its TID counterpart. These TIDs are sufficiently long such that a brute force attack could easily be detected and thwarted before it has any realistic chance of being successful. On Kit Check's tags, for example, the 96-bit TID factory locked memory bank includes a 48-bit unique serial number, representing over 281 trillion possible numbers.

By contrast, a serialized barcode is easy to copy and place on a second product's label by unsophisticated actors with relatively inexpensive equipment. And without a centralized registry, the downstream user has no easy way to be confident that the legitimate serial number is appearing on the correct product.

TID is one of the easier-to-understand technologies available on RFID tags today that can increase confidence in the product, but there are other technologies that can be employed too. The tag's *Lock* and *Kill* passwords can be used in such a way as to prove knowledge of a secret. The tag can also facilitate the use of secret keys, etc. And IC manufacturers can build in additional safeguards. Some tags manufactured by NXP, for example, offer authentication and privacy functions using AES and their *Brand Protection* feature which hardcodes certain manufacturer signatures into the chip's memory. Other sophisticated manufacturers offer similar technologies.

It's clear that the presence of TID and other technologies makes the RFID tag a more robust tool in the war against suspect and illegitimate products. Kit Check has been working with pharmaceutical manufacturers (and related service providers) to ensure they're laying the foundations around this technology so that we can begin using it in downstream validation checks beginning in 2020. We're confident this provides assurance unmatched by barcodes and by ecosystems void of an MDR, and we're excited to have just started opening up this technology to the industry.

Implications for Manufacturer Aggregation

If you combine the findings from Evaluations 13, 14, and 15, Sandoz work shows that performing aggregation with barcode vs. RFID costs the same. Given the additional downstream value from the presence of RFID tags, the total cost of ownership seems to clearly favor RFID-tagged items over barcode-serialized items.

Implications for Wholesalers

At the wholesaler, we see scenarios where a picker will get a 10-pack of vials for a customer's tote, but will barcode scan the wrong serial number or put the item in the wrong tote. By RFID-scanning the entire tote after it has been assembled, these risks can be eliminated, leading to more accurate distribution and data transmission.

Implications for Hospitals

Similarly, hospitals can receive totes and accurately qualify their contents, completing their required transaction records quickly. Further, they can extract additional value from the presence of that RFID tag by automating or improving other workflows throughout the hospital. For example, they can easily see their inventory down to the serialized unit dose level, which can be leveraged in the case of drug recalls for efficient, accurate, and complete handling.

Conclusions

DSCSA Is a Starting Point, Doesn't Need Ubiquitous RFID

In the children's game Telephone (or *Chinese Whispers*, for you Brits who are reading this), the first child creates a message and whispers it to the child sitting next to them. The second child then whispers it to the third child, and so on. When the message reaches the last child, it's said aloud and laughter ensues because the message inevitably gets garbled many times along the way.

DSCSA's product tracking requirements, and the handoffs of that data from one part to the next, feel a bit like the game of Telephone. Of course, supply chain participants will have a higher degree of accuracy than the children playing Telephone, but the very nature of this approach relies on a patchwork of disparate systems with many opportunities for errors to creep in and go completely undetected. Additionally, this patchwork approach makes it nearly impossible for hospitals to build systems that make use of this data in easy or universal ways.

DSCSA's current requirement that the serial number should only be applied to objects as granular as the saleable unit is also insufficient. It certainly helps enable traceability from the manufacturer to the hospital's loading dock. But as a hospital Director of Pharmacy recently told me, "that serial number is only good until it encounters a pair of scissors." In other words, once you break down that 10- or 25-pack of vials which had a serial number on the carton, and those vials get distributed and stocked throughout the hospital, there's no way to know which carton (and related serial number) each vial originated from. Tracking from manufacturer to loading dock is a start, but with the technology so readily available, we need to be thinking about this problem in a way that extends beyond the loading dock and to the patient to unlock the full set of opportunities around patient safety and inventory management efficiencies.

In a world where DSCSA defines these specific saleable unit serial number and product tracking requirements, you don't necessarily need RFID. You might want to use it in some scenarios, but you'll have to consider each situation and determine if there's a sufficient ROI. But as our Aggregation in Manufacturing explorations reveal, those ROI-neutral or -positive situations are more common than we might realize.

"Serialized Unit Doses" and a "Master Data Repository" is a Better Solution for Supply Chain Security

If we go back to first principles and think about what "supply chain security" should encompass, it's easy to see that we should be aiming higher than DSCSA's requirements, and our pharma manufacturing partners, such as Sandoz, agree. This year, we'll see tens of millions of unit doses shipping from Sandoz and others with serialized RFID tags embedded in the unit dose label, while still retaining the required serial number on the saleable unit. These numbers can easily be correlated in the MRD to understand the aggregation stack from top to bottom and, because there's a serial number on the unit dose, it can survive beyond the loading dock and that pesky pair of scissors. By having a serialized RFID tag on the unit dose, coupled with each drug's information in the MDR, this allows downstream stakeholders (hospitals, supply chain intermediaries, etc.) to build value-added software and services around the tag and data.

But will customers be willing to pay a little extra for the RFID tag? Many of these drugs are generics which leads to pricing pressures, so it's tempting to assume that customers won't be willing to pay a little extra. But, as Kit Check and other vendors have proven over the last 8 years, the market is increasingly recognizing the ***total cost of ownership*** of these products (not just their purchase price) and the value that each tag can bring, and they are continuing to change their buying behaviors accordingly.

All of this ultimately leads to a more efficient supply chain and increased patient safety. It makes aggregation activities in manufacturing facilities more accurate, which saves time, effort, and cost caused by rework activities. It allows hospitals to manage their inventory in more automated ways. It helps hospital staff quickly find all expiring, soon to be expiring, and recalled medications, solving the "needle in a haystack" problem. It allows EMRs to record the serial number of each unit dose administered, finally bringing full traceability from manufacturer to patient. And it allows for easy, automatic monitoring and detection of suspect and illegitimate products.

The Best Solution for Now: Saleable Unit Barcode + Unit Dose RFID

For 2020 and the near future, we believe that a hybrid approach is the most practical. All saleable units should continue to honor DSCSA saleable unit serial number requirements with a barcode. There is a large and vocal contingent of legacy supply chain participants who are looking to avoid cost and effort and will inevitably struggle to embrace certain innovations in the beginning, so this is probably all they can handle right now.

This "lowest common denominator" approach from them leaves great opportunities for those who are seeking to innovate, deliver even more value to our customers, and improve the safety of our patients. Manufacturers can opt in to unit dose tagging for specific NDCs that make sense, while maintaining the saleable unit barcode. They can start getting benefits from aggregation workflows immediately. And they can better meet hospitals' demands for products and technologies that truly deliver on better recall management, better detection of suspect products, and improved inventory management.

In the meantime, we'll continue building towards the ultimate solution, a world where each unit dose is serialized and supply chain participants have access to a single source of truth about each dose. In a world with this better solution, hospitals and patients will benefit from significantly improved data accuracy which leads to better patient safety, increased efficiencies throughout the supply chain, and better visibility into the lifecycle of each drug. This is a better way to solve the problems of supply chain security, and we have the tools to start doing this now.