Category / Specific items of compliance	Notes
Know Your Manufacturer's Brand Protection Team	
Close coordination between secondary online marketplaces and manufacturer brand protection teams are key to patient safety and the securing of the supply chain.	
For the top XXX products sold on the platform in the last 12 months, do the manufacturers of these medicines maintain logins and access to review sales listings on the platforms?	(confirm with brand protection teams, not platform)
Does the platform provide a portal or API through which brand protection teams can monitor transactions and listings?	
Does the platform maintain current product lists and brand protection contacts for every product sold or listed on the platform?	This one seems like it is something to ask the brand protection teams as well. Have they provided a product list and contact to the platform?
Does the secondary marketplace have an email address and a phone number for brand protection team members to notify the marketplace of a suspicious sale? Response should be within two business days.	Should we provide some guidance about how to signify a suspicious sale? Sometimes this will be up to professional judgement, but perhaps a few items such as non-matching GTIN and Serial?
Does the platform have the ability to verify genuine products with manufacturer brand protection teams?	Ideally, this would be via API, but a point of contact would also be helpful.
Know Your Products	
Using GS1 and DSCSA standards can help prevent diverted or counterfeit product from being sold through platforms.	
Does the platform require all participants registered on the platform to provide their unique location number (GLN) according to the GS1 standards as applied to pharmaceutical products?	
Does the platform record the unique identifying information (GTIN, SN, EXP, LOT) for all products sold on the platform according to the GS1 standards as applied to pharmaceutical products?	
Does the platform only show the unique identifying information for product listings (GTIN, SN, EXP, LOT) to the listing entity and the manufacturer's brand protection team and only those parties until the product is sold?	
Does the platform require the unique identifying information provided for by the GS1 standards before a sold product is shipped?	
Does the platform reveal the unique identifying information (GTIN, SN, EXP, LOT) for a product to the purchaser at time of purchase, and no earlier?	I think this is moot if we ask it be delivered at time of sale.
Does the platform allow the manufacturer's brand protection team to view unique identifying information for listings for six years, whether they were sold, unsold, or withdrawn?	
Does the platform require the unique identifying information provided for by the GS1 standards when a product is received?	Yes, the idea is that a purchaser would verify the unique identifying information on receipt of the product. We can't really *require* that the purcahser do this, but it should at least be possible to do.
Does the platform generate a transaction history record as required by the GS1 standards?	
Does the platform generate a record of the transaction statements for each transaction as required by DSCSA regulations, without relying on any of the exemptions provided by DSCSA?	

Does the platform generate transaction information as required by DSCSA regulations, without relying on any of the exemptions provided by DSCSA, and record in that transaction information the product identifiers provided for in the GS1 standards?	
Is the platform compliant with the requirements of the DSCSA when a transaction occurs that is not subject to an exemption such as named patient need or public health emergency?	The goal here is really to specify that the platform is compliant with DSCSA without relying on the exemptions. This may not be necessary, and the language may not reflect the intent, either.
Does the platform restrict access to the GS1 unique identifying information to the specific parties in a transaction?	
Does the platform disallow sale of products from lots that have been announced in recalls and counterfeiting	
Know Your Customer	
Modern diversion and counterfeiting rings adopt and shed corporate shells frequently to avoid accountability after their crimes are discovered. Online secondary marketplaces can help deter this behavior through rigorous identification of participants.	
Do the platform's terms and conditions require that that registered entities on the platform that are authorized to trade prescription medications are licensed to engage in these transactions by the relevant state and local authorities?	
Does the platform capture a participant's NPI number at registration time?	
Does the platform capture a participant's state license and DEA license at registration time?	
Does the platform capture a participant's NCPDP number at registration time?	
Does the platform capture a participant's contact information, including phone number at registration time?	
Does the platform have a know your customer (KYC) program it follows? Is that program documented?	
Does the platform verify that a business registered with the platform is in good standing with a valid bank account?	
Does the platform verify that any bank accounts registered with the platform are open, registered to an appropriate person/entity and able to engage in transactions.	
Know Your Policies	
Clear, enforced policies can discourage bad actors from using a platform to sell dangerous medicine.	
Does the platform require users, as a part of its terms and conditions, to comply with the requirements of the DSCSA, without relying on exemptions to the DSCSA?	Is this necessary, as compliance is legally required? Is it just there to provide something to violate as a condition of expulsion if violated?
Does the platform prohibit participants from scraping, downloading or otherwise using GS1 product identifiers for any purpose other than for bona fide transactions?	
Does the platform state clearly in its policies that it will ban an entity that lists or sells counterfeit medication for which it cannot provide a legitimate record of purchase from another entity?	
Does the platform state clearly in its policies that participants named as defendants in criminal complaints related to medicine safety, or civil complaints related to trafficking in trademark-infringing products will be suspended and/or banned?	
Does the platform's terms and conditions require platform buyers and sellers to notify the platform if their entity is named in a criminal, civil, or regulatory complaint related to trafficking in diverted or counterfeit medicine?	

Does the platform notify participants of its policies and that it monitors the site for suspicious behavior?	
Does the platform have a policy that requires participants to respond to inquiries about suspicious behavior?	
Does the platform keep records of all listings and transactions with associated GS1 identifiers for six years?	
Does the platform adhere to the following IT security practices:	
The marketplace must adhere to current, relevant IT security standards to prevent bad actors from infiltrating the platform or using DSCSA information for counterfeiting purposes.	[Is there an industry standard for this?]
Uses HTTPS for all production web interfaces.	Being able to assert this is problematic.
Requires secure user authentication to access all web interfaces capable of conducting transactions.	
Requires individual user accounts and prohibits sharing of accounts between individuals.	
Associates individual user accounts with licensed and registered entities.	
Requires API keys for all third-party access to APIs that contain listing information and/or permit conducting transactions.	
Uses firewalls for all production databases.	Being able to assert this is problematic.