Category / Specific items of compliance	Changes	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.		Summary: You should have a way of allowing brand protection teams to contact you (phone and email) and receive an answer within two business days about suspicious products offered for sale. You should create accounts in ten business days for brand protection teams to do listing surveillance either through the standard interface or a brand portal. Bonus: You should provide an API for brand protection teams to pull listing data from.
Does the platform provide a portal through which brand protection teams can monitor transactions and listings? OPTIONAL: Do they also provide an API?	Old language: Does the platform provide a portal ~~or API~~ through which brand protection teams can monitor transactions and listings?	Providing a portal is the minimum level of compliance.
Have drug manufacturers that have requested logins on the platforms to monitor listings and transactions received them within ten business days?	Old language "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? "	This will be confirmed with the brand protection teams and judged accordingly.
<Requirement deleted>	Old language: Does the platform maintain current product lists and brand protection contacts for every product sold or listed on the platform?	The burden for tracking their products should fall on the brand protection teams, and not require the platforms to maintain a list.
Does the secondary marketplace have an email address and a phone number for registered brand protection teams to notify the marketplace of a suspicious sale?	Old language: Does the secondary marketplace have an email address and a phone number for registered brand protection teams 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?
<Requirement deleted>	Old language: Does the platform have the ability to verify genuine products with manufacturer brand protection teams?	Because the platforms don't take possession of product, they are not an authorized trading partner. They should not be initiating product verification requests.
Know Your Products		
Using GS1 and DSCSA standards can help prevent diverted or counterfeit product from being sold through platforms.		Summary to do for compliance: Each product listing should capture the four DSCSA package ids (GTIN, LOT, EXP, SN) and store them privately with the listing's buyer, seller, and prices for six years. Listings should be kept for this duration whether completed, unsold, or withdrawn. Unique package identifiers should be disclosed to purchaser at time of purchase for shipment arrival verification. Listing information, if not available via portal, should be disclosed to product manufacturer protection team upon request within ten business days. No products identified by lot or serial number in recalls should be allowed to be sold. Sales of products should generate a DSCSA-compliant transaction history, information, and statement and store it for six years.
Does the platform record the unique identifying information (GTIN, SN, EXP, LOT) for all products listed for sale on the platform according to the GS1 standards as applied to pharmaceutical products?	Old language: 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?	To ensure people don't sell multiple units under one serial #, a listing should require entry of the identifiers at listing time, and not allow them to be changed. Even if delisted, the identifiers should be recorded and retained for six years.
Are product listings including buyer, seller, and prices and the GS1 identifiers associated with them stored for six years, whether sold, unsold, or withdrawn?		
<Requirement moved>	Old language: 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?	Moved to know your customer.
Does the platform allow the manufacturer's brand protection team to see the buyer, seller, prices, and unique identifying information for their products' listings (GTIN, SN, EXP, LOT) for the last six years on demand through a portal or within ten business days? This includes product listings sold, unsold, or withdrawn.	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?	
<Requirement deleted>	Old language: Does the platform require the unique identifying information provided for by the GS1 standards before a sold product is shipped?	If you have to provide it upon listing, then this isn't necessary.
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?		

<Requirement deleted>	Old language: 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?	Obviated by requirement above.
Optional: Does the platform allow purchaser of the product to confirm receipt of the same unique identifying information from the sale when sold product is received?	Old language: 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, without relying on any DSCSA exemptions, and store it for six years?		
Does the platform generate a transaction statement as required by the GS1 standards, without relying on any DSCSA exemptions, and store it for six years?		
Does the platform generate a transaction information as required by the GS1 standards, without relying on any DSCSA exemptions, and store it for six years?	Old language: 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?	
Duplicative of above requirement	Old language: 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?	Duplicative of similar requirement above
Duplicative of above requirements	Old language: 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 alerts from manufacturers or regulators?		
## 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.		Summary to do for compliance: Collect many official designations (NPI, GLN, NCPDP, license #'s, etc) at registration time. Have and follow a documented Know Your Customer program. Verify that businesses are in good standing and have active bank accounts registered to an appropriate entity.
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 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 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.		Summary to do for compliance: Ensure that terms of service / platform policies prohibit behavior that would endanger patient safety, so that violators can be banned from the platform, including: scraping GS1 product identifiers, being defendants in complaints related to supply chain safety or trademark infringement, failing to notify the platform that they are defendants in such cases, or failing to respond to platform or brand protection team inquiries about listings.
<Requirement deleted>	Old language: 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 Terms Of Service for the platform prohibit participants from scraping, downloading or otherwise using GS1 product identifiers for any purpose other than for bona fide transactions?		Can be used as a basis for termination from the platform.
<Requirement deleted>	Old language: 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?	Providing receipts is not a requirement.
Does the platform state clearly in its policies that participants named as defendants in criminal complaints related to medicine supply chain safety, or civil complaints related to trafficking in trademark-infringing medicines will be banned from the platform for their current and all future businesses?		
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 or medicine trademark infringement?		
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 from the platform or brand protection teams about listings on the platform within two business days or have their account suspended until the queries are answered?		
<Requirement deleted>	Old language: Does the platform keep records of all listings and transactions with associated GS1 identifiers for six years?	Obviated by requirement in another section.
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 unauthorized purposes.		Summary to do for compliance: Does the platform adhere to a number of IT security practices listed below? Does the platform have an external verifier of their security adherence, such as a third party audit or certification?
Uses HTTPS for all production web interfaces.		
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.		Only if you offer APIs.
<Requirement deleted>	Old language: Uses firewalls for all production databases.	covered by security standards
Can demonstrate external verification that the marketplace and IT systems holding sensitive data are compliant with an industry standard for security such as GAMP5, ISO 27001, FDA's Computer Software Assurance (DRAFT), or other industry standards for security and integrity.		