HMA WGEO Rapid Alert FormFalsified or illegal product found in the illegal supply chain

Unique Reference N0 (to be filled by Men Date: 07.04.2020 Time: Please complete sections 1 to 5 providing	Initials:	
1. REPORTING PERSON		
Name:	Position:	
Organisation:		
Address:		
Telephone	Ext:	
e-mail address:		
2. PRODUCT DETAILS		
Product name: Various products, including products related to COVID-19		
Manufacturer:		
Supplier: mainpharmacy.org and world-pharmacy.org		
Legal status: Banned ☐ Falsified ☑ Unlicensed ☑ Stolen ☐		
Dosage form: Various		
Strength: not known		
Batch / lot no: Is batch number genuine: Yes No		
If yes to the above, advise batch destination country:		
Expiry date: not known		
Language of packaging: not known, at least English		
Date of discovery: 26-03-2020		
Details of discovery:		
The 26 th of March the Dutch Health Care Inspectorate received intelligence		
about Dutch website who are being abused for the selling of illegal		
pharmaceuticals. This information is shared with the national Financial cyber		
team. After an investigation they concluded the Dutch websites are hacked		
due to non-updated plug-ins on the Wordpress websites. Besides this they		
also found out that the Wordpress software was not up-to date. The websites		
are guiding visitors to world-pharmacy.org and mainpharmacy.org.		

The illegal medicine sellers created subdirectories on each of the hacked websites.		
Technically it is not possible for the Financial cyber team to shut down the		
hacked websites, so they choose to call the host or owner and urge them to		
take that part of the website down or take down the complete website.		
In total it involves 71 infected websites all over the world.		
Some products offered on the websites are COVID-19 related, but also		
products in relation to erectile dysfunction and others.		
A report has been made of the investigation, for this moment only in Dutch. If		
one needs more information or wants to share information about this case,		
please do contact me by e-mail.		
It is not known since when these websites are hacked.		
Analysed: YES ☐ NO ⊠		
If yes, result of analysis:		
3. DISTIRUBUTION METHOD		
Internet: YES NO		
Internet:	Non internet, advise full details:	
URL: see supplier	Thorriternet, advise ruii details.	
Website address:		
Other details:		
Currency of payment:		
Has product reached patients/consumers? Not known. 4. RISK TO PUBLIC HEALTH		
Adverse reactions: YES NO \(\bigcap \)		
If yes, please advise details: take down a part of the websites or shut down the websites.		
Medical assessment details:		
5. NEED FOR PUBLICITY		
5. NEED FOR PUBLICITY Are you making a public statement? YES	<u></u>	
5. NEED FOR PUBLICITY Are you making a public statement? YES Are you issuing a press release? YES	 NO ⊠	
5. NEED FOR PUBLICITY Are you making a public statement? YES		

6. DISSEMINATION	
Are you content for this Rapid Alert to be shared outside WGEO membership?	
YES ⊠ NO ☐ (please see below)	
If yes, please specify which of the below you are content for this to be shared	
with (you may tick more than 1 box)	
Law Enforcement ⊠ Industry Security □ Trade Associations □	
Traders ☐ Customs (nominal data) ☐ Other ☒	
Please specifyPFIPC	
7. PHOTOGRAPH	
If possible, please attach a photograph of the product.	
See below.	



