While serialization in pharmaceutical and medical device packaging may be appropriate to identify or recall medicines with manufacturing or distribution problems, it cannot prevent the introduction of falsified medicine into the legal supply chain. By contrast, in order to increase reliability in the supply chain, digital authentication technologies that incorporate covert (invisible) security features provide a higher level of security than those with overt (visible) features; are easier and more cost-effective to deploy than those based on consumables; do not require any specific training, only a step-by-step process; and are more reliable than human sensory perception-based verifications. While the newly adopted European directive 2011/62/EU calls on pharmaceutical companies and any actors involved in the manufacturing or distribution of medicinal products to verify the authenticity of medicines, innovations in smartphone technology, including better image capabilities and increased computing power, will accelerate the need to develop a suitable, easy-to-use, and reliable product authentication process at the patient level.

When looking at the product security market, there are over 100 security technologies (holograms, digital watermarks, DNA taggants, serialization, etc.) used to combat counterfeiting of primary or second-
ary packaging and of solid or flexible components, such as liquids, powders and tablets. For a branded pharmaceutical manufacturing company, it is however challenging to understand the scope and role of each of these technologies, especially when considering the cost of the technology feature itself and its nationwide or worldwide deployment.

**Patient responsibility**

The basic question whether it should be left to patients to identify counterfeit Medicines is a topical issue both in developing and in industrialized countries, because consumer goods, including medicines – notably those not reimbursed by health insurance companies and those issued without a prescription (OTC – over the counter) – are increasingly purchased via the Internet. However, a study carried out by the European Alliance for Access to Safe Medicines found that 62% of medicines ordered on the Internet were substandard or counterfeit. Of these, 68% were unlicensed imitations and the rest were counterfeit branded medicines.

The question therefore arises as to the patient’s responsibility in determining the authenticity of medicines. Today, a number of Track and Trace applications (e.g. serialization, bar codes, RFID Tagging, etc.) are used in the pharmaceutical industry to prevent falsified medicinal products from entering the legal supply chain. According to the World Health Organization, these involve assigning a unique identity to each stock unit during manufacture, which then remains with it through the supply chain until its consumption. Using any cell phone, a patient can identify and send the unique serial number printed on secondary packaging via SMS text message to a central database. The serial number is then automatically confronted with a free or already used position. The diagnostic will be ‘authentic’ if the number was never sent before or possibly ‘fake’ if already checked. If the outcome is “fake”, the secondary packaging is either a counterfeit or a second use of the original packaging, filled with highly probable fake medicine.

With this technology, the patient is given full responsibility for verifying the authenticity or not of the medicine. The success of this procedure must however first rely on access to and utilization of mobile authentication devices, which could be problematic for elderly patients, people with motor restrictions or who are visually impaired, and patients affected by socio-cultural and economic inequalities, for example. It is then based on the impossibility of transferring the verification process to a pseudo-server in the hands of counterfeiters. In other words, man-in-the-middle (MITM) attacks. Finally, it depends on the reliability and accuracy of the written code sent by the patient via text message, provided that patients systematically check the serial number position. If not, genuine positions remain unchecked and vulnerable to counterfeiting.

Given these risks, patients should not bear the responsibility for uncovering fake medicine.

**Drug manufacturer’s role**

The next question arises as to the drug manufacturer’s liability in the event of a ‘false posi-
A false positive occurs when a counterfeit medicine is authenticated as genuine by the verification process, an outcome that might in turn affect a patient’s health. It is quite easy to imagine how such a false positive could be generated with this serial number verification: a batch of genuine medicine is hijacked somewhere in the supply chain and while the genuine tablets are removed and sold in bulk, the genuine packaging is filled with fake medicine. Or, imagine the following scenario: leaks, corrupt or coerced players in the supply chain create fake replications of medicine. In these cases, fake medicine will be authenticated as genuine and inadvertently reach the patient.

Claims that tracing the secondary packaging of medicine along the supply chain – in other words, creating its e-Pedigree – would prevent counterfeited medicine from entering the legitimate supply chain, are once again highly unrealistic. Nowadays, no major European pharmaceutical industry player would vote for such a complex tracking and tracing solution, because, according to reports, it would require “… major packaging line changes and investments” and true interoperability between medicine manufacturers, wholesalers and prescription deliverers. Although creating an e-Pedigree does provide valuable data on the history of a particular batch of drugs, it does not prevent fraudulent players in the supply chain from substituting genuine products with fakes and patients from purchasing them in turn.

Identification and authentication

The original goal of batch or individual serialization was a means to identify and recall medicines with manufacturing or distribution problems. Although integral to patient safety, trying to change the primary purpose of serialization into an authentication process is problematic. Logistically speaking, this technology forces pharmaceutical companies to print a visible linear bar code on the packaging or label, which can sometimes be difficult given the variable size of the printable area and the code/substrate contrast. In addition, inspections and controls must be in place to ensure that a unique code is applied on each individual pack or label. Moreover, serialization requires adaptive hardware, software and skills.

In the case of authentication, there are many security features available to brand owners and manufacturers capable of detecting counterfeits, not only with primary and secondary packaging, but also with dosage forms.

The most efficient features are covert, or invisible to the naked eye. According to the World Health Organization, “The purpose of a covert feature is to enable the brand owner to identify a counterfeited product. The general public will not be aware of its presence nor have the means to verify it”. These secret or covert procedures are widely available today and include invisible printing, embedded images, and digital watermarks, to name a few. These methods can help detect counterfeits by means of regular sample controls carried out at different points in the supply chain, even in the case of consumed or recovered packaging waste.

Some cost-effective, yet reliable technologies involve embedding an invisible marking on primary and secondary
packaging using regular visible ink and standard printing processes, without having to change the packaging design or flow of production. Another option involves using the intrinsic micro-differences present in a cavity mold commonly used to create vials or medicine containers, capturing an image of the random pattern, and then storing it in a database. In either case, the brand owner or manufacturer simply scans the item using a flatbed office scanner or an iPhone smart phone to receive a ‘genuine-or-fake’ outcome.

As a consequence, while serialization may be appropriate to identify basic fraudulent actions, such as extension of the expiration date or market diversion, it is not suitable to determine the authenticity of a medicine. Understandably, it would be challenging for anybody, even for customs or logistics employees, to detect a real medicine from a fake. It is an either-or situation: either the replica is so poorly done (fake brand name, spelling mistakes or other omissions) that there is no need to access the packaging information to determine that it is a counterfeit, or the replica is so well done that the visual inspection will lead to think that the packaging contains real medicine. A visual inspection of packaging by the human eye is therefore unreliable in identifying counterfeits.

**Remote online verification via the web will reduce the risk of leaks**

**Visual inspection**

Nothing looks more like a real medicine than a ‘well-made’ counterfeit, which is sometimes virtually indistinguishable from the original.

This fact is particularly problematic for customs employees and other players in the supply chain, whose job consists in reading or visually inspecting a packaging, whose different elements may or may not be correctly replicated by counterfeiters. Some of these systems convert the object into a 3D representation displayed on a computer screen.

**Verification features**

Digital solutions for product authentication are easier, faster and more cost-effective to deploy compared to security consumable-based solutions, especially when considering large production volumes. When selecting a security feature, it is not only important to assess the cost of purchase, implementation, global deployment and management, and resistance to replication, but also how a ‘genuine-or-fake’ verification is performed.

**Smartphones**

Smartphones are continuously evolving with increased functionalities and computing power, as well as image and video capabilities.

Smartphones can therefore benefit the development and expansion of digital authentication features based on invisible marking, allowing mobility and “on-the-fly” genuine-or-fake verification. However, these advancements do not mean that mobile verifications should be placed in the hands of patients, because of various unanswered questions raised earlier.