Adopting security features to protect pharmaceutical products against counterfeiting are becoming necessary and must not be confused with the adoption of serialization codes using barcodes or matrix codes or even RFID tags used to track and trace pharmaceutical products along the supply chain.

There are a number of ways able to uncover fake medicines, such as overt or covert security features requiring machine readable or human sensory ‘genuine-or-fake’ verification. Special attention should be devoted to identify the various costs that should be considered when deploying an anti-counterfeiting program worldwide and the processes available using software and digital imaging technology, instead of using additional security elements or security substances.

Anti-counterfeiting and traceability are different problems, requiring different solutions. On the one hand, traceability needs standardization and interoperability amongst the various manufacturers and the intervening third parties within the supply chain up to the dispensing point; on the other hand, anti-counterfeiting features, especially those invisible to the naked eye or covert ones, need secrecy and confidentiality. They should be constantly kept in pace with the technological advances of the counterfeiters. Nowadays hundreds of various anti-counterfeiting solutions can be identified with having each their proper domains of application. Protecting a folding carton packaging, an aluminium blister pack, a flexible packaging, a tablet, a liquid, a glass or polymer jar will call for different solutions. Selecting the right one for the right product is of the duty of the brand product manufacturer, not only considering the cost of the security feature but considering the global cost of the industrialization and the deployment of the anti-counterfeiting program worldwide.

Some countries have introduced or are planning to introduce pharmaceutical product traceability under government rules such as in Turkey, Brazil, USA or France. For example France will enforce by Dec. 31, 2010 the adoption of a batch serialization system based on human readable characters and an ECC 200 data matrix code using the GS1 – 128 coding. Two dimensional bar code readers should be in place in all pharmacies and points of passage of the medicines along the supply chain by January 2011.

The main issue of traceability systems is to increase patient safety, enabling for example, a rapid recall of suspicious batches. It also protects against basic fraudulent behavior, such as expiration date extension and reduces the risk of delivering wrong medicine to patients. Some projects have been based on the use of RFID tags, first recommended by the FDA (US Food and Drug Administration) in the mid 2000, but now abandoned because of the high price and its industrial feasibility, if considered at the dose level. RFID is more and more used in stores, warehouses and shipping areas for inventory control.

Pharmaceutical and regulation authorities have now clearly made the distinction between standardized track and trace solutions, which should increase patient safety in delivering the right dosage in the right place and authentication solutions to identify counterfeiting. This will remain the duty of the original pharma manufacturers to protect their IP and to stop counterfeiting of their medicines as early as possible, and at least before the counterfeit products reach the patient.

The naked eye

Many pharmaceutical companies have added visible security features to their packaging
to prevent counterfeiting. These include, for example, holograms, kinegrams, embossing, micro printing, moiré or special ink such as optical variable ink. However, these visible features provide not only minimal security, but they also require training for effective authentication when faced with fraudulent reproductions of such visible security features.

The use of ‘covert’ features invisible to the naked eye will produce a higher level of protection, due to the inability of counterfeiters to identify the presence of such features and they consequently cannot attack them. Covert security should never be disclosed and to prevent leaks they should only be known to a limited number of trustworthy persons.

The best known covert security solution is invisible ink, such as UV ink (visible under ultraviolet light) or IR ink (visible under infrared light). To authenticate these inks, a lamp which emits light in the required wavelength range will suffice. The drawback of these inks is that they can be bought by anyone very easily on the market. There are other chemical tracers or ink additives providing security against counterfeiting, such as DNA or magnetic tracers which provide higher security because relying on verification devices very difficult to get but from the original security feature provider.

The problem with such special inks, ink additives or taggant resides in the related logistics and manufacturing procedures, such as press cleaning, temperature and pressure sensitivity, as well as interaction with other chemicals. Although very efficient and effective, their implementation and deployment are quite costly.

All these techniques based on a security additive can be qualified as “analog or hardware based”, because they require additional security elements or special security substances.

Hardware and software

As in other industries, the digital or software revolution opens exciting new possibilities. Digital technologies can now be used to combat counterfeiting of pharmaceutical products at low cost while providing a high level of security. These digital technologies are breakthroughs compared to former methods.

Hardware and software

As in other industries, the digital or software revolution opens exciting new possibilities. Digital technologies can now be used to combat counterfeiting of pharmaceutical products at low cost while providing a high level of security. These digital technologies are breakthroughs compared to former methods.

Genuine or fake?

On selection of a security feature, it is not enough to just evaluate the purchase cost, the robustness against fraudulent replication, the cost of implementation in the production process, the cost of global management and any impact on the production process. An important part of the problem is how a ‘genuine-or-fake’ verification is performed.

In this case, the various anti-counterfeiting features can be placed in two categories:

- the features which use human sensory perception
- the features which are machine readable.

If human sensory perception is used (visual, tactile, oral), adequate training is required for a person to be able to distinguish a genuine security feature from a fake replication when both are to hand. While in the case of a machine readable feature, only a step by step process is required which, if it is well documented, can be performed by anyone without any specific knowledge or training.

Online and offline

For chemical or other ink additive security features, offline security processes are mainly carried out with specific scanners. In this case, achievement of verification programs at multiple sites requires the branded product manufacturer to purchase multiple scanners. The alternative would be that any suspected item be sent to a central location.

Example of ‘genuine-or-fake’ verifications based on digital imaging software using standard consumer electronics equipment which can be offline or online
for verification. Such a procedure would be quite costly and would considerably delay the expected ‘genuine-or-fake’ verdict.

Internet and mobile connections are today widely available around the world, including in the developing countries. A security feature enabling ‘genuine-or-fake’ verifications to be carried out online via a central secured server results in an almost instant verdict. This constitutes a major benefit, eliminating the need for sensitive security elements to be in the hands of an operator and thus avoiding the risk that retro-engineering be carried out on the equipment with a view to counterfeiting.

Another major benefit of an online verification is the consolidation of all the verifications performed worldwide, thus facilitating the detection of any correlation between various fraudulent sources within the supply chain. As for all criminal acts, the quicker you uncover them the more you are well positioned to identify the criminal source and can act to stop it.

Protecting packaging

The digital revolution mentioned above has generated numerous anti-counterfeiting solutions based on visible ciphered coding and invisible marking. One patented covert security solution uses just normal visible ink to protect various layers of pharmaceutical packaging. This solution protects already billions of items worldwide.

It uses a pattern made by apparently random micro dots invisible to the naked eye printed on the primary or secondary packaging or label (offset, flexography, rotogravure). These dots are invisible to the naked eye and spread over the whole surface of the packaging or label. The pattern is generated by a 128 bit software key big enough to offer billions of billions of different patterns, each one constituting a unique identity. The micro dots are very difficult to distinguish, even with a magnifying glass, as the dots’ color and size are chosen to be camouflaged within the imperfections found in all printed material structures.

For aluminum based blister packs, the patented solutions uses micro variations of the thickness of the lacquer layer in other words micro holes instead of micro dots. The varnish is applied by regular varnish printers (offset, flexography, rotogravure) without incurring additional production cost.

Accordingly, the invisible pattern of micro dots or micro holes can be easily integrated into any current packaging production line. The digital file of the security pattern is simply embedded in the prepress packaging artwork using standard graphic design software. It requires no modification of the packaging design and it is incorporated as usual before creation of the printing cylinder.

Protecting vials

A new, patented solution recently disclosed is based on the unique and intrinsic characteristics of the tooling used in the production of various medicine containers. With this solution, additional marking is unnecessary. The process detects and records the unique “signature” of microscopic surface irregularities created by the tooling or molds used for producing the parts. The process only requires the storage of a digital reference image or “template” of each mold used in the production of the molded parts. It follows that only a limited number of templates are necessary to authenticate the entire production of molded containers or other plastic parts. High tech digital imaging software is used for comparing the templates with the digital image of the surface of a suspicious part, which is produced by standard low cost office flatbed scanners.

Software based and digital security features can protect packaging and labeling, closures and vials against counterfeiting and has to be considered separately from serialization and track and trace features. Cost of deployment is fairly lower for software based security features compared to special substances or hardware based security elements.

Machine-readable security features enable any authorized person to carry out instant ‘genuine-or-fake’ verifications worldwide, with almost no prior training or any specific security knowledge. If online verifications are feasible, it allows instant consolidation of all ‘genuine-or-fake’ verification results performed anytime anywhere, thus maximizing the chances of uncovering fraudulent sources and putting a stop to them.