World Health Organization

IMPACT International Medical Products Anti-Counterfeiting Taskforce

20, AVENUE APPIA – CH-1211 GENEVA 27 – SWITZERLAND – TEL CENTRAL +41 22 791 2111 – FAX CENTRAL +41 22 791 3111 – WWW.WHO.INT

Anti-counterfeit Technologies for the Protection of Medicines

The attached draft text has been kindly prepared by Mr G. Power, Director, Packaging Security Global Quality Assurance, GlaxoSmithKline, on the basis of input from WHO and other parties, as well as his practical experience.

1. INTRODUCTION

There are a great many anti-counterfeit technologies available to manufacturers and brand owners, ranging from the very simple but effective, through to the highly sophisticated and extremely secure. The majority can be implemented on one or more of the packaging components, but some features can even be applied at the product level, either by direct marking or by using physical or chemical markers within the formulation.

The purpose of an anti-counterfeit feature is primarily to enable the authentication of an item, either by industry investigators, or ideally, by the wider public. The second function may be to act as a deterrent to anyone considering counterfeiting a product based on the difficulty or cost involved set against the likelihood of detection, and therefore prosecution. It must be stressed that security devices on packaging components provide no assurance as to the authenticity of the contents, which may have been substituted or adulterated. Security devices alone do not reduce counterfeits, but are designed to make them easier to detect.

Anti-counterfeit technologies can be broadly classified as follows:

- **Overt, or visible features**
- **Covert, or hidden markers**
- **Forensic techniques**
- **Serialisation/Track and Trace**

This paper will consider each of these 4 categories, whilst avoiding specific reference to any licensed product or provider. However, it must be recognised that some of these technologies are protected by international patents, and may only be available from licensed suppliers, subject to appropriate royalties or license fees. On the other hand, some can be applied in-house, with little expenditure on materials and effort, and most are available from reputable suppliers, some of whom specialise in security applications.

Note: *the following comments and conclusions must be viewed as very general to each group of technologies, and inevitably there will be exceptions with, and omission of, some more specialist applications.*

2. ANTI-COUNTERFEIT TECHNOLOGIES

2.1. OVERT (Visible) Features

Overt features are intended to enable end users to verify the authenticity of a pack. Such features will normally be prominently visible, and difficult or expensive to reproduce. It should be noted that overt features can add significant cost, may restrict supply availability, and require education of end users to be effective. Where overt features are used, experience is often that counterfeiters will apply a simple copy which mimics the genuine device, sufficiently well to confuse the average user.

They also require utmost security in supply, handling and disposal procedures to avoid unauthorised diversion. They should be applied in such a way that they cannot be reused or removed without being defaced or causing damage to the pack – otherwise genuine used components may be recycled with fake contents, giving a false impression of authenticity. For this reason an overt device might be incorporated within a Tamper Evident feature for added security.

2.1.1 Holograms

Probably the most familiar overt feature is the “dove” hologram which has been used to protect credit cards for many years. A hologram normally incorporates an image with some illusion of 3-dimensional construction, or of apparent depth and special separation.

Holograms and similar optically variable devices (OVD) can be made more effective when incorporated in a tamper evident feature, or as an integral part of the primary pack (e.g. blister foil). They can be incorporated into tear bands in overwrap films, or as threads embedded into paper substrates.

However, some hologram labels have been easily and expertly copied or simulated, and may often rely on hidden covert elements for authentication.

2.1.2 Optically Variable Devices (OVD)

OVDs also include a wide range of alternative devices, similar to holograms, but often without any 3D component. Generally they involve image flips or transitions, often including colour transformations or monochromatic contrasts.

Like holograms, they are generally made up of a transparent film which serves as the image carrier, plus a reflective backing layer which is normally a very thin layer of aluminium. Other metals such as copper may be used to give a characteristic hue for specialist security applications.

Extra security may be added by the process of partial de-metallization, whereby some of the reflective layer is chemically removed to give an intricate outline to the image, as can be seen on many banknotes. Alternatively the reflective layer can be so thin as to be transparent, resulting in a clear film with more of a ghost reflective image visible under certain angles of viewing and illumination. Partial removal of the metallic layer is a more restricted process and thereby increases both the level of security and the cost.

2.1.3 Colour shifting security inks and films

These can show positive changes in colour according to the angle viewing angle, and can be effective either as an overt graphic element or by incorporation in a security seal.

Colour shifting pigments are finely ground metallic laminates which need to be laid down in a thick opaque film to achieve the optical effect, and are therefore better suited to printing techniques such as gravure and screen printing rather than lithographic printing. Their security value lies in the specificity and dynamics of the colour change

(e.g. from blue to gold), combined with the difficulty and expense involved in manufacture. They are only available from a limited number of pigment suppliers, via a few specialist ink manufacturers. Positive authentication may involve forensic (microscopic) examination and embedded taggants.

Colour shifting films have been used for security applications, involving multi-layer deposition of thin films to build up a structure with unique diffractive properties, and vibrant colour transitions. They can be applied as security seals or tamper evident labels.

2.1.4 Security graphics

Fine line colour printing, similar to banknote printing, incorporating a range of overt and covert design elements such as guilloches, line modulation and line emboss. They may be used as background in a discrete zone such as an overprint area, or as complete pack graphics, and can be printed by normal offset lithography, or for increased security by intaglio printing. Subtle use of pastel “spot” colours makes the design more difficult to scan and reproduce, and security is further enhanced by the incorporation of a range of covert design elements, such as microtext and latent images.

2.1.5 Sequential product numbering

Unique sequential numbering of each pack or label in a batch can make counterfeits easier to detect in the supply chain. If printed visibly, it provides a semi-overt means of authentication by reference to a secure database, because duplicates or invalid numbers will be rejected. The main disadvantages of sequential numbering are that the sequence is predictable and easily replicated, and end users require some means of access to the database. The more secure option is serialisation by means of a pseudo-random non-repeating sequence, and this is discussed in the Track and Trace section (4).

2.1.6 On-product Marking

On-product marking technologies allow for special images or codes to be placed on conventional oral dosage forms. These overt technologies can be difficult to replicate and offer a security technology at the pill level. This added layer of security is effective even when products are separated from the original package.

General Conclusions:

Overt Features	
Advantages	**Disadvantages**
User verifiable	Require user education – not always widely understood
Newer technologies more secure	May be easily mimicked

Can add decorative appeal	May add significant cost
Can be a deterrent to counterfeiters	May rely on covert features for authentication
	May be re-used or refilled
	May give false assurance

Overt features represent an attempt to put authentication into the hands of the general public. However, to be effective they demand public education and awareness, which is especially difficult in the most challenged developing markets. It should also be noted that the more widely used one overt security technology becomes, the more attractive it is for counterfeiters to defeat it

2.2 COVERT (Hidden) Features

The purpose of a covert feature is to enable the brand owner to identify counterfeited product. The general public will not be aware of its presence nor have the means to verify it. A covert feature should not be easy to detect or copy without specialist knowledge, and their details must be controlled on a “need to know” basis. If compromised or publicised, most covert features will lose some if not all of their security value. For this reason such techniques will not be disclosed in detail in this paper.

Examples include:

2.2.1 Invisible Printing

Using special inks, invisible markings can be printed on almost any substrate, and which only appear under certain conditions, such as via UV or IR illumination. They can be formulated to show different colours with illumination at different wavelengths.

2.2.2 Embedded Image

An invisible image can be embedded within the pack graphics which can only be viewed using a special filter, and cannot be reproduced by normal scanning means. The effects can be quite dramatic, and yet well hidden.

2.2.3 Digital Watermarks

Invisible data can be digitally encoded within graphics elements and verified by means of a reader and special software. The data can be captured using webcam, mobile phone or other scanning equipment, but the digital information is not visible to the human eye, and attempts to replicate it will be detected by virtue of the degradation of the embedded data.

2.2.4 Hidden Marks and Printing

Special marks and print may be applied in such a way that escapes attention and is not easy to copy. Their effectiveness relies on a combination of secrecy and subtlety, and hence no further details will be discussed here.

2.2.5 Anti-copy or Anti-scan design

Fine line background patterns appear as uniform tones, but when scanned or copied reveal a latent image which was not previously visible. Commonly used on secure documents to prevent photocopying, they may be applied to product packaging as a background tint.

2.2.6 Laser Coding

The application of batch variable details by lasers coding requires special and expensive equipment, and results in recognisable artefacts which may be difficult to simulate. Laser codes can be applied to cartons and labels, and plastic and metal components.

2.2.7 Substrates

There are many ways of incorporating covert markers within a substrate, such as visible or UV fluorescing fibres, or chemical reagents in carton board or paper. Watermarks can be embedded in leaflet paper, or metallic threads interwoven in the base material, possibly including an overt OVD feature. These require a dedicated supply source and large volume production, which, if affordable, results in a very effective option.

2.2.8 Odour

Micro-encapsulated distinctive odours can be applied as an additive to an ink or coating to provide a novel covert or semi-overt feature.

General Conclusions:

Covert Features	
Advantages	**Disadvantages**
Can be simple and low cost to implement	Need strict secrecy – “need to know”
Needs no regulatory approval	If widely known or used, may be easy to copy
Can be easily added to or modified	More secure options add supply complexity and cost

Can be applied in-house or via component suppliers	If applied at component suppliers, greater risk of compromise

Covert features are most effective in the hands of industry specialists. They are a very valuable investigative tool, but a counterfeiter will be able to copy many of the simpler features unless they are skilfully applied and their details are kept secret. However, there is almost unlimited scope to the possibilities, given imagination and ingenuity on the part of the technologist and designer, and the costs can be minimised or even eliminated when applied in-house. In-house application also has advantages of limiting involvement of third party suppliers, who may not be trustworthy in some environments. Only the most secure covert features can be safely used in an overt context, and these generally come under the next heading of **forensic markers**.

2.3 FORENSIC Markers

There is a wide range of high-technology solutions which require laboratory testing or dedicated field test kits to scientifically prove authenticity. These are strictly a sub-set of covert technologies, but the difference lies in the scientific methodology required for authentication.

Examples include:

2.3.1 Chemical taggants

Trace chemicals which can only be detected by highly specific reagent systems, but not normally detectable by conventional analysis.

2.3.2 Biological taggants

A biological marker can be incorporated at extremely low levels (parts per million or lower) in product formulations or coatings, or invisibly applied to packaging components. At such low levels they are undetectable by normal analytical methods, and require highly specific “lock and key” reagent kits to authenticate.

2.3.3 DNA taggants

Highly specific DNA “lock and key” reagent systems can be applied to packaging by a variety of printing methods. They require a “mirror image” recombinant strand to effect the pairing, and this reaction is detectable by a dedicated device. Security is further assured by hiding the marker and reagent pair in a matrix of random DNA strands, but the test is tuned to work only with one recombinant pair.

2.3.4 Isotope ratios

Naturally occurring isotopes can be highly characteristic of the source of a compound, and accurately determined by laser fluorescence or magnetic resonance techniques. These can provide a "fingerprint" of one or more of the product constituents, or alternatively a specific marker can be added with its own unique signature. Detection requires highly specialist laboratory equipment

2.3.5 Micro-taggants

Micro-taggants are microscopic particles containing coded information to uniquely identify each variant by examination under a microscope. This may take the form of alphanumeric data depicted on small flakes or threads, or of fragments of multicoloured multilayered laminates with a signature colour combination. These can be embedded into adhesives, or directly applied to packaging components as spots or threads.

General Conclusions:

Forensic Technology	
Advantages	**Disadvantages**
High tech and secure against copying	Licensed technologies usually limited to one source
Provide positive authentication	Significant cost
May be disclosed for overt purposes	May be difficult to implement and control across many markets
	Wider use increases risk of compromise
	Unlikely to be available to authorities or public

There are some very robust and secure options available, which may enable their use to be more widely known and therefore accessible to trusted authorities and investigators. However, these tend to be subject to patent protection and therefore restricted in availability and pricing.

2.4. Serialisation/TRACK and TRACE Technologies

A number of Track and Trace applications are under development for the pharmaceutical sector, although the principles have been established for many years in other contexts. These involve assigning a unique identity to each stock unit during manufacture, which then remains with it through the supply chain until its consumption. This identity will normally include details of the product name and strength, and the lot number and expiry date – although in principle it may simply take the form of a unique pack coding which enables access to the same information held on a secure database.

(This latter solution overcomes some of the concerns about privacy where the encoded data can be read at a distance by radio equipment.)

These serve a number of distinct functions:
(a) Tracking an item through the supply chain, to each point where there is the facility for data capture.
(b) Providing traceability on the history of any item (electronic pedigree), subject to limitation of number of control points.
(c) Enable authentication of the data at any time, and by implication, of the pack or unit on which it is applied.

The most obvious benefits are in the supply logistics, where greater transparency of inventories and demand patterns can lead to efficiency improvements and cost reductions. Another benefit is the ability to identify a product through to dispensing to the patient, enabling the elimination of medication errors and the ability to speedily recall defective product batches. But the ability to tightly control and authenticate all product through the supply chain greatly reduces the possibilities for counterfeit, stolen or diverted product entering the distribution system without being detected.

It should also be noted that Track and Trace tags or labels may not necessarily be applied at the unit pack level, but may be restricted to whole cases or even pallets – thereby affording the logistics benefits but not all the safety and security gains. As has been mentioned before, a key security element lies in pack serialisation.

2.4.1 Serialisation

In itself the Track and Trace label may not be immune to copying or falsification, but its security is greatly enhanced by the inclusion of unique and apparently random serialisation, or non-sequential numbering, ideally at individual item level. If the serialisation was sequential, then the level of security would be very low as the sequence is predictable, whereas “random” serialisation using a highly secure algorithm or method of encryption overcomes this. Individual packs may still be copied, but the database will identify duplicates or invalid serials, as well as those which have been cancelled or expired, or which appear in the wrong market, or with invalid product details.

Where secure serialisation is applied visibly to a pack, then it may be authenticated by customers via a telephone or internet link to the database. One issue to be resolved is ownership, management of and access to the database, to ensure that the information is readily accessible and yet secure against compromise.

There are two main vehicles for the incorporation of unique pack data in order to facilitate automatic data capture:

2.4.2 Bar Codes

These are high-density linear or 2 dimensional bar codes incorporating product identity down to unit pack level, which are scanned and referenced to the central database. One popular implementation is the 2D datamatrix code, and other possibilities include

PDF417 codes. A 2D code can typically be 1cm square or smaller, and yet contains up to 1 Kb of data with some "redundancy" or error correction. Where space is not a limitation, linear bar codes may also be used. The codes are printable by on-line methods including inkjet or digital printing, allowing direct computer control and transfer of records to the central database. Hierarchical systems are developed whereby the label on a shipping case is inextricably linked to the identities of all its contents, and this can further extend up the chain to pallet labels, thereby overcoming the necessity for line of site scanning through the supply chain.

So-called "nano-printing" technologies allow microscopic application onto individual tablets. UV inks allow invisible printing onto any substrate including glass vials and ampoules.

2.4.3 Radio Frequency Identity (RFID) Tagging

An RFID tag comprises of an antenna with a microchip at its centre. This contains item-specific and batch information which can be interrogated at a distance, and without requiring line of sight (unlike bar codes). The radio frequency used determines the range and sensitivity, but no one specification suits all applications. Some systems are able to capture multiple records for a mixture of different products, but there are some issues around orientation of the tags and absorbance of the radio signal by liquids and foils. But one clear advantage of RFID is that it has the potential to be fully automated in warehouses and even through to pharmacies, without requiring manual intervention.

Specifications for equipment and data standards are being developed. The cost of tags remains a significant barrier to individual pack application, as does the availability of the application and verification equipment if it is to be implemented to pharmacy level. Robustness of the tags during application and handling through to end of life is another issue, as trials to date indicate a significant failure rate. However there is optimism that a printed version may be developed. Privacy issues, and susceptibility to deliberate adulteration must also be addressed prior to widespread implementation.

2.4.4 Unique surface marking or topography

There are several methods for applying a pseudo-random image to each item in a batch, such as a pattern of lines or dots in one area of the carton, and then scanning the signature into the batch database via secure algorithms, for later authentication. Alternatively, the pack surface provides a unique fingerprint when scanned by a dedicated laser device, which enables each pack to be registered into the database at batch manufacture, and which is impossible to replicate or falsify.

General conclusions:

Serialisation/Track and Trace	
Advantages	**Disadvantages**

High tech and secure against copying	Significant cost to implement and monitor
May be capable of remote authentication, via phone or internet	Difficult to implement across multiple markets
May be accessible to authorities and investigators without compromise	May be vulnerable to hackers
May eliminate dispensing errors	Damaged labels may not read
Facilitates recall of defective product	Robustness of RFID tags not proven
May combat theft and fraud	Needs harmonisation of standards
Benefits in supply efficiencies	Not accessible to the public
	Remote reading causes privacy issue

Unique pack serialisation has the potential to deliver robust solutions to fraud and counterfeiting of pharmaceuticals, but is not yet fully developed. Barcode systems use proven existing technology, but lack the advantage of automation and remote scanning possible with RFID. But RFID systems are not yet proven or robust, and standards need to be agreed and defined. RFID tags may be vulnerable to deliberate and invisible alteration or corruption.

3. SUMMARY and CONCLUSIONS

As can be seen above, there is a huge range of possible solutions ranging from the very simple to the highly complex, from zero cost to highly expensive and from fragile to highly secure against compromise. The wide range of options adds to the potential security by diluting the advantage gained by a counterfeiter in defeating any one system, and manufacturers should choose widely and wisely for optimum security gain.

It is unlikely that any one solution will be appropriate for all applications - the costs may not be affordable in developing markets, or for low margin products including generics and OTCs.

Pharmaceutical manufacture is not restricted to highly developed and sophisticated societies, but is almost universal. Therefore, not all areas share the same accessibility to technological solutions, and their supply infrastructure. It is also noted that reliable and secure sources of supply may be wanting in some regions where there is a poor history of intellectual property protection. Manufacturers may be confined to using only in-house technologies in such territories.

Virtually all of the available solutions carry some cost and administrative burden, whereas the manufacturers' business case for cost versus benefits is extremely difficult to quantify. This is not helped by many unsubstantiated claims for the level of counterfeits in the global medicines market. The true business case is more realistically based on risk management and corporate ethical responsibility for public health and safety, except in those few areas where the counterfeit level is measurable.

Finally, there is no single solution to every problem, and a secure strategy will almost certainly involve a mixture of technologies, often in combination. An overt feature will almost certainly include a secure covert element for added security, and any one product may carry several different features on various levels of the pack and components. But as long as counterfeiters target medicines for illegal profit, a product with no form of anti-counterfeit marker represents a significant potential risk to public health and safety.

3.1 Overt user-verifiable solutions would be the ideal option, if only they were universally robust, affordable and readily understood by end users. Some licensed technologies claim to achieve this, but mandating the use of these would be counter-productive. They may not be suitable for all applications, nor affordable by all manufacturers for all products, and their wider use would become a greater incentive to counterfeiters to invest in engineering the technology, as has happened with holograms.

Recommendation: *overt features should only be used at the discretion of manufacturers. Their use should be encouraged where products and/or markets are known to be at risk, and where used, manufacturers should educate the public (including wholesalers, distributors and healthcare professionals) in the means by which they can be authenticated. There is little purpose in mandating the use of an overt solution, as counterfeiters will be obligated to attempt to defeat or to circumvent it.*

3.2 Covert solutions have much to offer manufacturers, but offer little benefit to authorities and the general public because of the risk of compromise if widely known or widely used. However, they can be very cost beneficial and relatively simple to manage.

Recommendation: *Manufacturers should be encouraged to apply covert markers across their entire range of products and markets, to provide a basic means of monitoring the situation. Wide use of one or two simple features should be discouraged however, as the risk of compromise increases for all, and they should not be relied upon alone to solve an ongoing problem of counterfeiting. Manufacturers should consider sharing knowledge of some covert markers with trusted supply chain partners.*

3.3 Forensic markers have some advantages over the simpler covert features, but generally at a cost premium, both in terms of licensing fees or royalties and the equipment required. Their security may be sufficiently robust to allow overt advertisement of their presence, and they may bridge the gap between less secure covert features and unreliable overt features.

Recommendation: *the use of forensic markers should be encouraged in areas of high risk, and once a manufacturer has committed to a system there may be advantage in wider use across their portfolio for little extra cost. However, choice of system must be at manufacturers' discretion and any attempt to mandate a solution must be discouraged.*

3.4 Serialisation/Track and Trace systems differ by not necessarily being secured against copying, but by protecting the supply chain against infiltration and abuse. They also have additional benefits of safety, and the improvements in supply logistics and efficiency suggest that they may be self financing before even taking into account safety issues and counterfeit elimination. There is good reason to believe that a common database structure will support any of the proposed implementations, whether 2D barcode or RFID. RFID shows promise, but there is a long way to go before it is proven, reliable, affordable and practical in all markets. It should also be recognised that the problem of counterfeiting is greatest in markets where the IT infrastructure needed to support Track and Trace is most lacking, and the traders in counterfeits have no incentive to encourage its development.

Recommendation: *manufacturers and healthcare providers should be encouraged to the platforms, standards for and practicalities of implementing Track and Trace technology. Establishment of specifications for the data structure and database infrastructure are essential platforms to harmonisation of a universal system. Principles of ownership, management and access must be agreed, and the modes of access made as flexible as possible. The choice of hardware platform should be left to manufacturers, but it is recommended that for speed and economy a barcode based system should be developed as a priority, allowing natural progression to RFID if, when and where feasible. RFID tagging may be more effective at pallet and case level, but 2D barcodes more affordable at individual pack level. An industry wide working group should be established to define the standards, with representation from branded and generics manufacturers, wholesalers, distributors, pharmacists and healthcare practitioners. Consideration should be given to how access might be afforded to authorities such as customs, police and public health investigators, as well as ultimately to the customer.*