Appendix 2

AVAILABLE AUTHENTICATION TECHNOLOGIES FOR THE PREVENTION AND DETECTION OF SSFFC MEDICAL PRODUCTS

TABLE OF CONTENTS

I. INTRODUCTION ................................................................. 16
II. OVERT (VISIBLE) TECHNOLOGIES ........................................ 18
   II.1. Tamper-evident measures ............................................ 18
   II.2. Holograms ............................................................ 20
   II.3. Optically variable devices .......................................... 21
   II.4. Colour shifting security inks and films .......................... 21
   II.5. Fugitive inks .......................................................... 22
   II.6. Security graphics ..................................................... 23
   II.7. Scratch-off technologies ............................................ 23
   II.8. Overt use of a covert technology .................................. 23
III. COVERT (HIDDEN) TECHNOLOGIES ..................................... 24
   III.1. Invisible printing ..................................................... 24
   III.2. Latent image or three-dimensional (3D) intaglio printing .... 26
   III.3. Embedded image .................................................... 26
   III.4. Watermarks or filigrees ............................................ 26
   III.5. Digital watermarks .................................................. 26
   III.6. Hidden marks ........................................................ 27
   III.7. Microtext or microprinting ......................................... 27
   III.8. Anti-copy or anti-scan designs ................................... 27
   III.9. Safety fibrils or filaments ......................................... 27
   III.10. Laser coding ........................................................ 28
   III.11. Marks in a die-cut profile ........................................ 28
   III.12. Substrates ............................................................ 28
   III.13. Odour ................................................................. 28
IV. FORENSIC/CHEMICAL MARKERS ......................................... 28
   IV.1. Chemical taggants .................................................... 28
   IV.2. Biological taggants .................................................. 29
   IV.3. DNA taggants ......................................................... 29
   IV.4. Isotope ratios ........................................................ 29
   IV.5. Micro-taggants ........................................................ 29
V. TRACK AND TRACE MODELS AND TECHNOLOGIES .................... 29
VI. DETECTION MODALITIES AND TECHNOLOGIES ...................... 30
VII. CONCLUSIONS ............................................................... 31
I. INTRODUCTION

1. Substandard/spurious/falsely-labelled/falsified/counterfeit (hereinafter SSFFC\(^1\)) medical products\(^2\) pose significant risks for public health. Preventing and combating actions, activities and behaviours that result in SSFFC medical products requires ongoing cooperation among numerous stakeholders, including national and/or regional regulatory authorities (hereinafter NRRA), justice representatives, law enforcement officials, customs authorities, pharmaceutical companies, distributors, repackagers, technology suppliers, health care providers and patients.

2. The security of the pharmaceutical supply chain can be strengthened by innovative packaging technologies and better business practices. Further, as stakeholders at points along the supply chain use new and innovative technologies, it is imperative that both those making policy/strategy decisions and the end-users understand the capabilities and limitations of existing authentication technologies.

3. At the third meeting of the Member State mechanism on SSFFC medical products, it was decided to establish a working group comprising Member States’ experts to survey the technologies, methodologies and “track and trace” models, in place and to be developed, in order to analyse their advantages and disadvantages; and to survey the available authentication and detection technologies and methodologies in order to analyse their advantages and disadvantages. At its fourth meeting, the Member State mechanism accepted document A/MSM/4/3, entitled “Existing technologies and ‘track and trace’ models in use and to be developed by Member States”. With reference to other elements of the mandate for Activity C, Member States were encouraged to share their experiences in using authentication and detection technologies and methodologies, and it was agreed that the mandate for Activity C would be extended by one year in order to complete the work.\(^3\)

4. The appearance of SSFFC medical products undermines confidence in genuine medical products. It can lead to recalls and liability suits to marketing authorization holders not involved in the actions, activities or behaviours that result in those products. From an industry perspective, product loyalty could be compromised as consumers perceive additional risks when using a particular company’s product. Implementation of effective authentication technologies may avoid this as well as ensure patients’ safety. The implementation of these technologies is seen as one of the most prominent preventive measures. In addition to providing authentication, they make the production of a convincing falsified drug more difficult and costly. Government authorities, by employing these technologies, may ensure that drugs in the supply chain are genuine.

5. In effect, the purpose of these technologies is primarily to enable the authentication of any sample, either by NRRA, industry representatives and other government officers or, ideally, by the wider public. The second function may be to act as a deterrent to anyone considering production of SSFFC medical products, based on the difficulty or cost involved set against the likelihood of

---

\(^1\) For the purpose of this document, SSFFC will be used in accordance with reference to the footnote in resolution WHA65.19 (2012): “The Member State mechanism shall use the term ‘substandard/spurious/falsely-labelled/falsified/counterfeit medical products’ until a definition has been endorsed by the governing bodies of WHO”, and the current document will not prejudge any further negotiation in relation to the definition within the Member State mechanism on SSFFC medical products.

\(^2\) For the purpose of this document, the term “medical products” will be used in accordance with paragraph 3 of document A/SSFFC/WG/5, which refers to “medicines, vaccines and in vitro diagnostics” and footnote 1, which reads, “This may also include medical devices at an appropriate time in the future.”

\(^3\) See document A/MSM/4/10, paragraph 10.
detection, and therefore prosecution. Some authors affirm that an ideal authentication technology should: possess a high level of security (non-clonable), higher product application and authentication speed, proven standards, be difficult to remove and reapply, be easy to check, have automatic authentication, be useable by consumers, and be legally compliant with regulation by the industries.

6. Authentication of a medical product and packaging may require the use of numerous features incorporating varying levels of technological complexity and product understanding. There are a great many authentication technologies available to manufacturers, 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.

7. Available literature delineates these features into four basic groups:

1. Overt, or visible features.
2. Covert, or hidden markers.
3. Forensic/chemical techniques.
4. Track and trace models and technologies.

8. Visual analysis, the simplest authentication methodology, is most aligned with overt features of both the medical product and/or packaging. These generally are considered to be visible to the naked eye. Visual analysis of covert features (such as microprinting and taggants) typically requires the aid of some device (e.g. microscope or hand-held reader) or may require some level of chemical analysis (e.g. chemical analysis of inks, packaging materials and dosage forms). Forensic/chemical analyses include chemical, physical or forensic tests that are conducted in a laboratory setting, or in the field utilizing portable instrumentation or specially deployed systems. It should be noted that portable instrumentation can be used both in the field and in a laboratory setting. Track and trace analyses utilize bar-coding or other forms of serialization (e.g. batch number and batch expiry) to ensure the pedigree of a product and require a database to be used for comparison. These models and technologies were already assessed in document A/MSM/4/3 entitled “Existing technologies and ‘track and trace’ models in use and to be developed by Member States”.

9. This document will review the first three categories, while avoiding specific reference to any licensed product or provider. It is worth mentioning that the available options described throughout the text are only illustrative. They are non-exhaustive and are based on information provided by countries, industry representatives and/or bibliographic references, the sources of which were not verified, and are, therefore, subject to change and/or rectification, as appropriate, with no other purpose than that of serving as a reference to Member States’ NRRA. The conclusions shall be viewed as very general, and there will probably be exceptions with, and omission of, some more specialist applications. This aims to be a “live document” that is updated on a periodic basis and in alignment with advances and new technologies development. See the attachment to this appendix for a summary of advantages and disadvantages.

10. On the other hand, it must be recognized that some of the technologies may be protected by international patents, and may only be available from licensed suppliers, subject to appropriate royalties or license fees. Also, some can be applied in-house, with little expenditure on materials and effort, and most are available from reputable suppliers, some of whom specialize in security
applications. Additionally, the applicable technologies for examining each of these features are generally different and may require specialized knowledge, experience and technical expertise.

11. The use of one or more of these technologies may be optional for manufacturers as well as they may be mandatorily required by NRRA regulations. When considering to adopt such technologies, in all cases, it is advisable to look at their costs, which vary from country to country and, therefore, a generalization cannot be made at a global level.

II. **OVERT (VISIBLE) TECHNOLOGIES**

12. These technologies are intended to enable patients and health care professionals to verify the authenticity of a medical product. They are visible to the naked eye and normally difficult or expensive to reproduce. Overt technologies require education of end-users in order to be effective. When overt technologies are applied, it is often the case that criminals trying to imitate the medical product may apply a simple copy that mimics the genuine device sufficiently well to confuse the average user. It should also be noted that the more widely used an overt security technology becomes, the more attractive it is for criminals to overcome it.

13. Overt technologies also require utmost security in supply, handling and disposal procedures to avoid unauthorized diversion. They should be applied in such a way that they cannot be re-used or removed without being defaced or causing damage to the pack and its components – otherwise genuine used components could be recycled with fake contents, giving a false impression of authenticity. For this reason an overt device should be incorporated within a tamper-evident feature for added security.

14. The following are examples of tamper evident features as well as available overt technologies.

**II.1. Tamper-evident measures**

15. Tamper-evident/tamper-resistant packing is packaging that has an indicator or barrier to entry which, if breached or missing, should provide visible or audible evidence to consumers that tampering has occurred (e.g. film wrappers, shrinkable seals and bands, breakable caps, tape seals, blister packs and hot melt).

16. Some of the commonly used tamper-evident measures are listed below.
17. Tamper-evident microcut labels: these labels are made of polypropylene, have micro cuts and are placed on the closure flap of the packaging. The patient and health care professionals must verify that the security seal is present and not damaged. The manufacturer logo can be added to the label, as well as other authentication measures, such as holograms. It is advised to instruct patients and health care professionals to verify the presence and integrity of this label by adding the text “DO NOT USE IF SAFETY SEAL IS ALTERED OR DAMAGED” in the medical product packaging.

Some of the typical micro cuts:

18. Tamper-evident VOID labels: these are labels that, once peeled off, transfer the legend “VOID” onto the surface of the container packaging, leaving clear evidence of the opening, and preventing the seal from being re-adhered without removal becoming evident. It is possible to manufacture personalized VOID in which a company logo or a different expression such as “OPEN” or “GENUINE PRODUCT” can be placed on the transfer adhesive.

19. Multi-destructible (“eggshell”) vinyl labels: these labels are made of a material that destroys itself into small parts if an attempt is made to peel them off.
II.2. Holograms

20. Also known as a “three-dimensional image” or a “dynamic image”, a hologram normally incorporates an image with some illusion of multidimensional (usually 3D) construction, or of apparent depth and spatial separation. If the hologram is moved, two or more overlapping images can be seen. Holograms can combine three-layered security features and constitute a powerful weapon against falsifying.

21. Holograms and similar optically variable devices 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. In effect, holograms may provide overt first-line authentication while covert features such as scrambled images, microtext, UV-sensitive or other specialized inks provide second-line authentication for trained examiners and appropriate decoding equipment.
II.3. **Optically variable devices**

22. Optically variable devices include a wide range of alternative devices, similar to holograms, but often without any three-dimensional (3D) component. They usually involve image flips or transitions, often including colour transformations or monochromatic contrasts.

23. Like holograms, they are generally made up of a transparent film that 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.

24. 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. 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 the level of security. There can be three security levels: a first level verifiable by the naked eye, a second level verifiable by portable instruments, and a third level verifiable by laboratory analysis and/or instruments.

II.4. **Colour shifting security inks and films**

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

26. Colour shifting pigments are finely ground metallic laminates that 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 green to red), combined with the difficulty and expense involved in their manufacture. They are only available from a limited number of pigment suppliers, via a few specialist ink manufacturers. Positive authentication may require microscopic examination.
27. 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.

II.5. Fugitive inks

28. These technologies consist of inks sensitized to water, alcohol, chemical reagents and other physical eradication. Upon contact with these agents, they disappear or suffer deformities, spots or light fluorescence. They are normally used in plane offset printing backgrounds.
II.6. Security graphics

29. These technologies imply 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.

II.7. Scratch-off technologies

30. This technology consists of a layer of removable ink by “scratching” with a fingernail or a coin, which once eliminated reveals a verification code. This code should be randomized, so that criminals cannot predict the codes that will be used. In addition, it must be checked against a database to verify if the product is authentic. This database could be administrated by the marketing authorization holder, the NRRA or another Government authority.

II.8. Overt use of a covert technology

31. Some of the covert technologies assessed below may be used in an overt context by advertising their presence. This only works if the technology is inherently secure against compromise and the end-users have the means by which to authenticate them.
III. COVERT (HIDDEN) TECHNOLOGIES

32. The purpose of a covert feature is to enable NRRA and marketing authorization holders (also other stakeholders in the supply chain who have knowledge of such technologies, as appropriate) to identify SSFFC medical products. Patients will not usually be aware of its presence nor will they 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 publicized, most covert features will lose some, if not all, of their security value.

33. Covert features are most effective in the hands of industry and NRRA specialists. They are a very valuable investigative tool, but criminals will be able to copy many of the simpler features unless they are skillfully applied and their details kept secret. However, there is almost unlimited scope regarding the possibilities, given imagination and ingenuity on the part of the technologist and the designer, and the costs can be minimized or eliminated where 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.

34. The following are examples of available covert technologies.

III.1. Invisible printing

35. Using special inks, invisible markings that only appear under certain conditions can be printed on almost any component. These markings cannot be viewed with the naked eye; a “developer” is needed in order to reveal the ink.

36. These inks should be liquid, suitable for writing, revealed by physical or chemical methods, invisible to white light and infallible when revealed. The “developers” include ultraviolet or infrared light, heat, cold and iodine vapour.

37. Luminescent ink is not visible within the white light spectrum. This group can include both fluorescing and phosphorescing inks. Fluorescent ink has a fluorescing pigment that can be seen when exposed to ultraviolet light of a specified wavelength. Blue short wave ultraviolet fluorescent ink is widely available and provides only a low level of security unless well hidden. Other colours (yellow, green or red) are more secure, and some combinations produce different colours with short and long wavelengths of ultraviolet light. Ultraviolet-suppressing pigment may also be added to render substrates non-fluorescing, or may be printed over a fluorescing background for subtle effect. Phosphorescent inks are those that continue to emit light for a short period of time after exposure, and can be detected with a reading device.
38. Reactive inks, unlike fluorescent inks, when subjected to ultraviolet light, vary in colour, but these colours are mat and non-fluorescent.

39. Infrared fluorescing pigments can be tuned to very specific wavelengths of invisible light, and are only available from specialist suppliers. They have a high security level.

40. Chemical reagent systems can be based on simple litmus type acid/alkaline reactions, but more secure systems utilize highly specific chemical reagents.

41. “Rub and reveal”/“coin reactive” inks are invisible until activated by rubbing with a coin. These inks merge with the application substrate and, once applied and dried, they can be wiped with a metal object such as a coin, after which the printed text acquires a gray colour that makes it readable to the naked eye.

42. Photochromic inks change colour when exposed to a specific wavelength of light. They have a high security level if detected via a specific reader.

43. Thermosensitive or thermochromic inks, disappear or change colour at varying temperatures (for example, the temperature of human skin). Once the stimulus has disappeared, they regain their colour or condition.
44. Some of the above can be more discretely applied for extra security by interspersing them within an apparently random patterning alongside a non-reactive pigment that has the same colour in normal light. When the reactive ink changes colour or fades away owing to the stimulus of temperature or radiant energy, it reveals an image or message that was obscured by the patterned background.

III.2. Latent image or three-dimensional (3D) intaglio printing

45. These are images that, to be displayed, need to be revealed. They are composed of horizontal and vertical lines that form, for example, letters, figures or logos. They are revealed according to the angle of incidence of light that, when it hits lines reveals opposed lines arranged otherwise.

46. They are made with chalcographic printing systems and cannot be copied by flat photocopy systems. The relevant issue is that the image must be able to be seen in a unique position – not in any other one.

III.3. Embedded image

47. An invisible image can be embedded within the pack graphics that can only be viewed using a special filter, and cannot be reproduced by normal scanning means. In its simplest form, this may involve “dot shift” displacement of part of a halftone element, but more sophisticated techniques include a scrambled image that is reassembled by a lenticular filter. The effects can be quite dramatic, and yet may be well hidden, for example, in a varnish coating or even a material substrate. Special software is used to create the embedded image and place it into the digital artwork.

III.4. Watermarks or filigrees

48. Their name derives from their fine grain. These features are placed on the paper/cardboard at the time of manufacture and before drying, causing a decrease in the thickness of the paper in the last stage of manufacture.

49. They are multi-tone or bitonal and can be localized or random. The pressure made by the nuances produces different degrees of weakening; these physical changes in material originate from a greater difficulty in transposing light.

III.5. Digital watermarks

50. Invisible data can be digitally encoded within graphics elements and verified by means of a reader and special software. This can be achieved remotely 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.
III.6. **Hidden marks**

51. Special marks may be printed in areas that are not normally visible, such as on carton glue flaps, and in a way which does not attract attention and is not easy to copy. Other examples include specialized print screens, e.g. stochastic or diamond screening.

III.7. **Microtext or microprinting**

52. Very fine text, down to 1 point letter size or below, that cannot be viewed with the naked eye, can be easy to incorporate in artwork, either within a pack design or as an off-pack feature, to aid verification. This is normally visible under low power magnification (x8), but with specialist printing techniques the text can be extremely small, requiring medium to high power magnification (“nanotext”). Microtext can be concealed by printing against a poorly contrasting background, or resembling a keyline or a complex path in a geometric design element.

53. With this type of letter, a legend or an entity or institution name are usually reproduced without interruption. Its implementation requires adequate capacity and technology (making it difficult to be reproduced) and it is not possible to photocopy, scan or reinsert, as it suffers damage that is impossible to repair.

III.8. **Anti-copy or anti-scan designs**

54. Halftones are normally printed as dot screens for continuous toning, but if fine parallel line patterns are used to achieve a uniform density or tone, these can be resistant to scanning or copying by revealing a secondary pattern that was not otherwise visible. Commonly used on secure documents to prevent photocopying, it may be applied to product packaging as a background tint.

III.9. **Safety fibrils or filaments**

55. These features are small visible or invisible white light fibrils, which are incorporated into the packaging material mass (e.g. cardboard or paper), intertwined with their most fundamental fibres. They consist of 5 mm synthetic threads (usually nylon) and can be of different colours. They can be distributed throughout the packaging or located in a specific part of it.

56. They can be detected by ultraviolet light, revealing different colours according to the material. They are placed when manufacturing the paper, so that criminals will be limited to copy them. Imitation safety fibrils may be printed or adhered to packaging material but never within its mass, except where criminals are able to develop their own cardboard/paper material.
III.10. Laser coding

57. The application of batch variable details by laser coding requires special and expensive equipment and results in recognizable characteristics that may be difficult to simulate. It generally involves burning away the characters from a dark printed panel via a stencil. Laser codes can be applied to cartons and labels, aerosol valves and plastic and metal components, enabling these to be identified.

III.11. Marks in a die-cut profile

58. The cutting die of a carton or label can be discretely modified to include cuts, nicks or altered corner radii in a carefully controlled manner, providing hidden markers that are unlikely to be noticed or copied, and yet are easy to verify. Punching or laser burning of a pattern of small holes is a variant used in some specialist applications.

III.12. Substrates

59. There are many ways of incorporating covert markers within a substrate, such as visible or ultraviolet 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 optically variable device feature. These require a dedicated supply source and large volume offtake, which, if affordable, result in a very effective option.

III.13. Odour

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

IV. FORENSIC/CHEMICAL MARKERS

61. There is a wide range of high-technology solutions that require laboratory testing or dedicated field test kits to provide scientific proof of authenticity. These are strictly a subset of covert technologies, but the difference lies in the scientific methodology required for authentication. It is important to ensure that such markers/taggers do not affect or impact the integrity of the product and are non-toxic.

62. There are some very robust and secure options available, which may enable their use to be more widely known and therefore accessible to NRRAs as well as other relevant investigating authorities.

63. The following are examples of available forensic/chemical techniques.

IV.1. Chemical taggants

64. These technologies are trace chemicals that can only be detected by highly specific reagent systems, but not normally detectable by conventional analysis.
IV.2. Biological taggants

65. 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.

IV.3. DNA taggants

66. Highly specific DNA recombinant “lock and key” reagent systems can be applied to packaging by a variety of printing methods. They require a “mirror image” strand to effect the pairing, and the 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 of strands.

IV.4. Isotope ratios

67. Naturally occurring isotopes can be highly characteristic of the source of a compound, and accurately determined by the use of various types of mass spectrometry.

IV.5. Micro-taggants

68. 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 multi-coloured, multilayered laminates with a signature colour combination. These may be embedded in any part of the medical product, in the adhesives, or directly applied to packaging components as spots or threads.

V. TRACK AND TRACE MODELS AND TECHNOLOGIES

69. Track and trace/traceability models, together with authentication technologies, support the integrity of the medical product. Their implementation has been identified by NRRAs over recent years as a useful and efficient tool to fight against the actions, activities and behaviours that result in SSFFC medical products. At the global level, some Member States have issued traceability regulations that have been implemented or are in the process of being implemented; others are assessing various implementation alternatives or otherwise have not approached the topic.

70. As these initiatives were considered relevant and a priority for Member States, at the third meeting of the Member State mechanism on SSFFC medical products, it was decided to establish a working group comprising Member States’ experts to assess and report on “track and trace” technologies, methodologies and models currently in use or under development, and analyse their advantages and disadvantages. As a result of the working group’s deliberations, document A/MSM/4/3 entitled “Existing technologies and ‘track and trace’ models in use and to be developed by Member States” was accepted by the Member State mechanism at its fourth meeting. Since the work was already done in relation to these models and technologies, no additional comments should be made about this issue.

VI. DETECTION MODALITIES AND TECHNOLOGIES

71. There are several ways to detect SSFFC medical products, ranging from the visual analysis of overt technologies described above to full chemical analysis in a laboratory setting. In the area of chemical analysis, a wide range of technologies are also available, spanning portable devices and full forensic laboratories. While laboratories can provide the most complete analysis, some portable devices have been shown to accurately identify SSFFC medical products in a high percentage of samples tested. The use of detection technologies should not be limited to dosage form medical products and should include active pharmaceutical ingredients and excipients. The role of detection technologies at the patient and health professional level is also important and needs further exploration.

72. As already stated above, visual analysis is the simplest detection methodology and is mostly related to the overt technologies described. This analysis usually implies the organoleptic observation of the product with the naked eye, but notwithstanding that, a visual analysis of covert technologies can also be performed with the aid of some device (e.g., microscope or hand-held reader).

73. Even in the absence of specific authentication technologies, it is always possible to identify SSFFC medical products by observation, measurement or analysis. For example, tablet weights and dimensions are tightly controlled and characteristic for any given formulation, making SSFFC medical products easy to detect by their inconsistency with the genuine product. To some extent this may also be true of the physical appearance and characteristics of the packaging components, especially where these are tightly specified and controlled by the manufacturers. Errors in artwork (text or graphics) are, however, more reliable indicators in view of the high standards to which licensed manufacturers operate.

74. For the analysis of covert authentication technologies, a greater degree of expertise, knowledge, and specialized equipment may be required to perform the examination and evaluation.

75. Forensic/chemical analyses include chemical, physical or forensic tests that may be conducted using field detection devices/technologies or in a laboratory setting. These analyses may be utilized in the examination of the entire dosage form and/or packaging material. There are numerous testing technologies, physical and chemical, that are designed to provide evidence that a product is SSFFC. Some examples include chromatographic and spectroscopic tests, chemical-induced colour-based testing, hardness and dissolution tests.

76. Chemical analysis conducted using methods and technologies available to a NRRA or the manufacturer and that assess the composition of a suspect product are often the most definitive way to authenticate it. Increasingly, however, many instrument companies are looking for ways to innovate these technologies to be more cost effective and user friendly. For example, less expensive, portable instrumentation that is easy to operate is becoming more readily available. Such portable/hand-held instruments can assist NRRA, law enforcement officers and customs officials in screening suspect samples at remote locations or ports of entry. In most cases the results generated by a field portable device are considered preliminary and may require confirmation through quality control laboratories.

77. In addition, compendial methods to assess identity, potency, or impurity profiles (i.e. monograph methods) may also provide a means by which suspect samples are authenticated. It should be noted that the identification and/or potency of the active pharmaceutical ingredient in a suspect dosage form is not sufficient to determine the authenticity of a suspect product.
78. Currently, several organizations, such as, for instance, the Asia-Pacific Economic Cooperation, the United States Pharmacopeia and the Infectious Diseases Data Observatory are working on assessing available field detection technologies. The outcomes of such ongoing work could be very useful for the purposes of this working group.

VII. CONCLUSIONS

79. There is a wide range of available authentication technologies to be implemented in medical products, 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 minimizing the advantage gained by criminals in overcoming any one system.

80. These technologies may be voluntarily applied by manufacturers or mandatorily required by NRRA. Nearly all of the available solutions carry some cost and administrative resources, which should be taken into account by NRRA.

81. All in all, there is likely no one guaranteed solution, and therefore 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 a medical product may carry several different authentication technologies on various levels of the pack and components.

82. Overt user-verifiable solutions would be the ideal option, if only they were universally robust, affordable and readily understood by health care professionals and patients. 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 are they affordable by all manufacturers for all products, and their wider use would become a greater incentive to criminals to invest in engineering the technology.

83. The use of such technologies may be encouraged where products and/or markets are known to be at risk, and, where used, health care professionals and patients should be properly educated in the means by which they can be authenticated.

84. Covert solutions have much to offer manufacturers and NRRA, but offer little applicability to the general public because of the risk of compromise if widely known or widely used.

85. Forensic/Chemical markers have some advantages over the simpler covert technologies, but they may usually imply a higher cost, 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 technologies and overt technologies.
## ADVANTAGES AND DISADVANTAGES

<table>
<thead>
<tr>
<th>Overt (Visible) Features</th>
<th>Covert Technologies</th>
<th>Forensic/Chemical Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advantages</strong></td>
<td><strong>Disadvantages</strong></td>
<td><strong>Advantages</strong></td>
</tr>
<tr>
<td>Patient and healthcare professionals verifiable</td>
<td>Require healthcare professionals and patient education (Not always widely understood)</td>
<td>Increase security measures by adding hidden features</td>
</tr>
<tr>
<td>Easy to locate and check</td>
<td>May be easily copied</td>
<td>May need no regulatory approval</td>
</tr>
<tr>
<td>It can add decorative appeal</td>
<td>May be re-used or refilled</td>
<td>If applied at component suppliers, greater risk of compromise</td>
</tr>
<tr>
<td>Can be easily added to or changed</td>
<td>May provide a false sense of security</td>
<td>Can be easily added to or changed</td>
</tr>
<tr>
<td>It can be a deterrent to criminals trying to illegally reproduce the genuine product</td>
<td></td>
<td></td>
</tr>
<tr>
<td>May also include covert features for authentication</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---