American Journal of Immunology

Research Note

Methods for Universal Authentication of Medical Devices

[1,2,3]Mark A. Brown, [3]Ilham Alshiraihi, [4]Callie Blase, [5]Joachim Storsberg and [5,6]Christian Schmidt

[1]Department of Clinical Sciences, Colorado State University, Fort Collins, CO 80523-1052, USA
[2]Epidemiology Section, Colorado School of Public Health, Fort Collins, CO 80523-1052, USA
[3]Cell and Molecular Biology Program, Colorado State University, Fort Collins, CO 80523-1052, USA
[4]Department of Marketing, Colorado State University, Fort Collins, CO 80523-1052, USA
[5]Department of Biomaterials and Healthcare, Division of Life Science and Bioprocesses, Fraunhofer-Institute for Applied Polymer Research (IAP), 14476 Potsdam-Golm, Germany
[6]Editorial Office, The American Journal of Immunology, S-207, 244, 5th Avenue, New York, NY, 10001 USA and S-71, 1A, 400, King William St, Adelaide, SA 5000, Australia

Article history
Received: 22-05-2019
Revised: 28-05-2019
Accepted: 15-06-2019

Corresponding Author:
Christian Schmidt
Fraunhofer Institute for Applied Polymer Research, Potsdam, Germany; The American Journal of Immunology, New York, NY, USA and Adelaide, SA, Australia
Email: schmidt102@gmail.com

Abstract: The need for effective means of authentication of medical devices has increased with the growing number of falsified *in vitro* diagnostics and devices being introduced across world markets. Such substandard products result in negative consequences ranging from harm to patients and/or failure to impart the desired clinical outcomes to a loss of public trust in healthcare providers and regulatory agencies. Herein, we discuss the growing specter of medical device falsification, related cybersecurity threats and selected novel approaches suggested for authentication.

Keywords: Medical Device, Cybersecurity, FDA, Health Disparities

Introduction

A medical device is defined as "...an instrument, apparatus, implement, machine, contrivance, implant, *in vitro* reagent, or other similar or related article, including a component part, or accessory which is: recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them, intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or intended to affect the structure or any function of the body of man or other animals and which does not achieve any of its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of any of its primary intended purposes" (Federal Food, Drug and Cosmetic Act; Allport-Settle, 2010).

The Food and Drug Administration (FDA) Center for Devices and Radiological Health (CDRH) is responsible for regulating the manufacturing, packaging, labeling and import of medical devices to be sold in the United States (US). The corresponding and harmonized regulatory framework for medical devices in Europe is known as the Medical Device Directive (MDD). Collectively, such regulatory frameworks throughout the world have, along with the World Health Organization (WHO), identified noteworthy safety issues resulting from an apparently ever-growing number of falsified medical devices, available across a range of world markets. Taking into account the acute need for sufficient cybersecurity, illustrated by a potential exploitation and/or manipulation of devices, compromised by malicious cyberthreats (World Health Organization, 2018), mounting evidence illustrates these insufficiently addressed needs and provide a powerful motivation for combined efforts to address these areas of concern.

More and more reports seem to indicate a considerable percentage of forged medical devices in low-income countries, with developed countries equally confronted with this issue (World Health Organization, 2018). Worldwide, it is estimated that at least 8-10% of all medical devices are fraudulent (Surat, 2018; World Health Organization, 2018) with low-income countries carrying the bulk of that burden (World Health Organization, 2018).

Despite its rigorous regulatory standards, approximately 5% of the US medical device market is comprised of fraudulent products (Glass, 2013; Nighswonger, 2003; World Health Organization, 2018; Fig. 1 and 2).

Estimated Percentage of Fraudulent Medical Products

Worldwide	United States
10%	5%

Primary Countries/Regions of Origin

China	Taiwan
Russia	Hong Kong

Annual Loss in U.S. Export Market for Medical Devices †

$6.4 B

† *In vitro* diagnostics, elector-medical apparatus, irradiation apparatus, surgical and medical instruments, surgical appliances and supplies, ophthalmic goods

Fig. 1: Estimates related to the percentage of fraudulent medical products, the documented primary countries/regions of origin for counterfeit products and the annual loss to the U.S. export market for medical devices

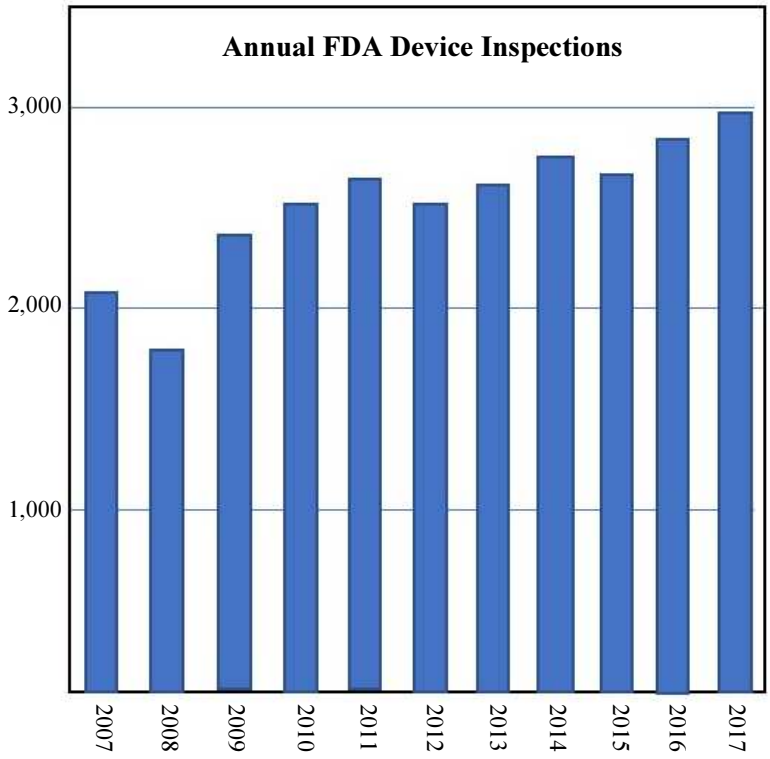

Fig. 2: FDA device inspections increased by 46% Between 2007 and 2017

Although the black market for inauthentic devices is widespread, a recent study pointed to verifiable sources, such as China, Russia, Taiwan and Hong Kong, although this is not to be construed as the origin of those devices, because criminal energy limits the illumination of the involved gray and even black markets (Nighswonger, 2003). As for the U.S. export market alone, a recent report estimates an annual loss of $6.4B for medical devices (International Trade Administration, 2016).

Discussion

Counterfeit medical products can be traced as far back as the 1600's with the documented emergence of a black market for fraudulent variations of cinchona bark, which was highly desired for its anti-malarial properties (Glass, 2013) with an even greater threat to health and international markets again in the 1800's with the emergence of adulterated or inferior forms of purified quinine (Glass, 2013). The list can be expanded and we refer interested readers to recent reports (International Trade Administration, 2016).

Counterfeit products span the breadth of medical devices from those with dental applications to surgical products. Among the most common targets include surgical mesh, bandages, gauze, contact lenses and thermometers. Failure and/or contamination of any of these can result in potentially serious harm to a patient. However, there has been a recent spike in truly life-threatening issues and consequent deaths associated with an alarming increase in the number of inauthentic devices for implantation such as plates, screws and spinal implants. Complicating the issue is the fact that counterfeiting is being conducted not only at the level of finished goods but also in the parts that are ultimately assembled into the final product. Thus, legitimate manufacturers may unintentionally release products that contain fraudulent components. For example, over $7M in intra-aortic pumps have been recalled due to improper functioning of what were revealed to be counterfeited components. In some cases, the manufacturers may be aware of the inauthenticity and become complicit in schemes to reduce costs and maximize profits. There is, perhaps, no better example of this than the PIP breast implant scandal, in which a manufacturer intentionally introduced sub-standard silicone into implants, resulting in inordinately high rates of implant rupturing and the recall of tens of thousands of implants (Vogt, 2012). Perhaps more disturbing is the vulnerability of connected medical devices for which there is little or no security from cyberthreats. These include a host of diagnostic equipment, such as CT scanners and MRI equipment, as well as critical therapeutic devices such as patient monitors, defibrillators and infusion pumps. This past year, the U.S. Department of Homeland Security issued new warnings related to the vulnerabilities of connected medical devices to potential cyberattack and the FDA recalled almost 500,000 Abbott pacemakers after it was discovered that those devices could be hacked and remotely controlled.

In direct response to the growing threats associated with medical devices, FDA increased its vigilance. With over 21,000 medical device manufacturers across 106 countries that are registered with the FDA, the agency conducts thousands of inspections of medical device manufacturing sites each year. Indicative of the increasing global nature of manufacturing medical devices is the fact that although there has been an impressive 46% increase in the number of annual device inspections by FDA in past decade, there has been a staggering 243% increase in the number of annual foreign device inspections during that same period. The agency has enhanced the efficiency of its efforts by instituting a risk-based approach to enforcing the most critical areas of concern.

However, while FDA surveillance may discourage fraudulent practices related to commercial medical devices, it cannot independently eliminate such issues, nor mount sufficient defense against growing cybersecurity threats. Thus, due diligence with regard to authenticity and cybersecurity is a responsibility of the global commercial medical device community, including end-users.

For medical devices, such emerging reports of using longer DNA fragments (Storsberg, 2018) gain traction and interest, although usage of this technology across platforms depends on further refinement. This aligns well with end-user approaches, such as sponsor-mediated approaches for authenticity (Su and Stolterman, 2016), or multi-factor authentication for cybersecurity (Sinha *et al*., 2019). That such sponsor-mediated and end-user approaches remain underutilized represents one of the greatest threats to patient safety and consumer confidence for the medical device industry. The need for universal authentication and security, along with a user-friendly method of adopting them, is recognized along with the urgent need to further the cause of authentication methods.

Author's Contributions

Mark A. Brown: Wrote the first draft of the paper.

Ilham Alshiraihi, Callie Blasé, Joachim Storsberg and Christian Schmidt: Provided critical input and assisted in revising and improving the paper. All authors read and approved of the final manuscript.

Ethics

MAB, IA, CB, JS and CS report no conflicts of interest with regard to this report. CS is a member of the

Editorial Board of The American Journal of Immunology and is waived from the Article Processing Fee for this contribution.

References

Allport-Settle, M.J., 2010. Federal Food, Drug and Cosmetic Act: The United States Federal FD and C Act Concise Reference. 1st Edn., PharmaLogika, Willow Springs, NC, ISBN-10: 098307190X, pp: 670.

Glass, B.D., 2013. Counterfeit drugs and medical devices in developing countries. Reports Tropical Med., 5: 11-22.

International Trade Administration, 2016. Top markets report-medical devices. U.S. Department of Commerce.

Nighswonger, G., 2003. Pursuing counterfeit medical devices. MDDI.

Sinha, A., G. Shrivastava and P. Kumar, 2019. A pattern-based multi-factor authentication system. Scalable Comput. Practice Experience, 20: 101-112.

Storsberg, J., M.K. Volkert, O. Mauger, M.A. Brown and C. Schmidt, 2018. Forgery-proof marking of breast implants by means of encapsulated DNA. Plastische Chirurgie, 18: 84-86.

Su, N.M. and E. Stolterman, 2016. A design approach for authenticity and technology. Proceedings of the ACM Conference on Designing Interactive Systems, Jun. 4-6, Brisbane, QLD, Australia pp: 643-655. DOI: 10.1145/2901790.2901869

Surat, P., 2018. Anti-counterfeiting technology for biomaterials. Med. Life Sci. News, 10: 1-4.

Vogt, P.M., 2012. PIP implant scandal backgrounds and consequences. CHAZ, 13: 37-41.

World Health Organization, 2018. Substandard and falsified medical products. WHO Home/News Fact Shee ts.