Medical devices in the disclosure era and the role of medical writers

Raquel Billiones
Clinipace Worldwide, Zurich, Switzerland

Correspondence to:

Raquel Billiones
Chriesbaumstrasse 2
CH-8604 Volketswil / Zurich
Switzerland
rbilliones@clinipace.com

Abstract

Increased transparency is one of the provisions of the Clinical Trial and Medical Device Regulations. This article discusses the impact of transparency and disclosure on medical devices. Many modern-day medical devices are software-driven. These, as well as the patients implanted with or wearing these devices, have become part of the so-called Internet of Things, and are therefore vulnerable to cyber attacks. Disclosure of information, data, and documents pertaining to medical devices will increase this vulnerability. In the rapidly changing regulatory landscape, the role of medical writers in anonymisation of patient data takes on a whole new magnitude. It is not only about protecting patient privacy, it is about ensuring patient safety.

Disclosure and devices

2016 was a big year for transparency and disclosure, starting with the release of the EMA Policy 0070 (*External guidance on the implementation of the European Medicines Agency policy on the publication of clinical data for medicinal products for human use)*[1] in March (and an update in December) and the public posting of the first redacted clinical reports in October.[2] As we come to grips with the impact of disclosure on the documents we write, we should not forget that clinical trials do not only involve drugs, but also medical devices. Devices are also subject to regulations that provide for increased transparency.

There was a time when clinical research and regulations on drugs and devices were considered worlds apart. If we consider the definition of a medical device as "*any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination… which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means*",[3] this separation is not surprising. Over the years, however, drug-device combinations and drug delivery systems (ranging from insulin pumps to drug-eluting stents to nicotine patches) have been developed, and the delineation between drugs and devices used in healthcare has become blurred. A quick look at the database on EUDRACT will show many current clinical trials that involve devices. And regulations that govern drugs and devices are slowly but surely being aligned.

In the rapidly changing European regulatory landscape, the EU Clinical Trials Directive was revamped and replaced by the 2014 Clinical Trial Regulation (CTR). This year, the EU Medical Device Directive is going to be superseded by the Medical Device Regulations (MDR).[3]

But what does this have to do with disclosure and medical writing? Like the new CTR, the new MDR also requires increased transparency of clinical data, with some selected documentations made available to the public. Below are extracts from the February 2017 MDR draft[3] on the topic of transparency:

- "(4) Key elements of the existing regulatory approach, such as the supervision of notified bodies, conformity assessment procedures, clinical investigations and clinical evaluation, vigilance and market surveillance should be significantly reinforced, whilst provisions ensuring transparency and traceability regarding medical devices should be introduced, to improve health and safety.
- (43) Transparency and adequate access to information, appropriately presented for the intended user, are essential in the public interest, to protect public health, to empower patients and healthcare professionals and to enable them to make informed decisions, to provide a sound basis for regulatory decision-making and to build confidence in the regulatory system.
- (48) For implantable devices and for class III devices, manufacturers should summarise the main safety and performance aspects of the device and the outcome of the clinical evaluation in a document that should be publicly available."

The exact implementation of the MDR provisions is still unclear. But if the MDR transparency requirements closely follow those of the CTR, we may see implementation guidelines that will resemble the EMA Policy 0070.[1] This means that many of the medical device clinical documents we routinely write, ranging from the clinical investigation report to the clinical evaluation report, may be required to be posted for public access.

Dangers of disclosure

One of the main weaknesses of disclosure is the risk of patient re-identification. It has been demonstrated that anonymised personal and medical data, the type we collect in clinical trials and registries, can actually be used to re-identify individual patients, threatening their privacy and the confidentiality of sensitive personal data.[4]

In the world of medical devices, the risks that disclosure brings do not just stop at invasion of privacy but take a more ominous form – an attack on a device that is implanted in the patient. This endangers the patient's life. Hence, disclosure of CT documents dealing with medical devices does not only present a risk to patient privacy but also a major risk to patient safety.

Implantables and wearables

In the era of personalised medicine, there is nothing more "personal" than a device implanted in a patient. Implantables can range from stents to hip replacements to an artificial heart. Then there are the wearables (no, not iWatch and Google Glass), devices worn for diagnostic and therapeutic purposes. These range from hearing aids to continuous glucose monitoring (CGM) devices. The individual devices ("units") are highly specific to the patient wearing the unit ("users"). Each unit is identified by a serial number and can provide metrics that are specific

to the users. For example, there was the case of the pacemaker that gave away its user in an arson case. At the exact time of the fire on his property, the device did not record any cardiac activity indicative of stress or excitement expected under such circumstances. This pointed to a deliberate setting of fire by the wearer of the pacemake.[5] Then there was the case of the patient whose CGM system data revealed a deliberate overdose delivery of insulin by the user.[6]

On the flipside of the coin, identifying an implanted or a worn medical device from information such as device model, manufacturer, bar code, or serial number can lead to de-anonymisation of an anonymised patient. An additional complexity comes from the fact that many modern-day medical devices are software-driven, making patients wearing devices such as implantable cardiac defibrillators (ICDs) or insulin pumps a part of the so-called Internet of Things (IoT). Being in the IoT makes these devices vulnerable to hacking and breaches.

Hacking the heart helpers

In a review of medical device cybersecurity, Burns et al.[7] presented theoretical scenarios of murders committed by manipulating a pump to deliver the wrong insulin dose or re-programming a pacemaker to give incorrect pacing – remotely. Unlikely? Earlier this year, the US FDA issued a safety communication on the cyber vulnerabilities of a radio frequency-enabled ICD and the corresponding transmitter.[8]

Breaching the ER

Cyber attacks and hacking are not only restricted to portable devices. Large medical devices in clinics and hospitals, from the simple electrocardiogram to the more complicated body scanners and surgical robots are all run by software. Again, being in the IoT, these devices can be breached by an experienced hacker hundreds of miles away.[9]

Regulations on cybersecurity

Regulatory authorities recognised these threats and are coming up with measures to mitigate them.

The US FDA has released two industry guidelines on medical device cybersecurity:

- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices; Guidance for Industry and Food and Drug Administration Staff 2014
- Postmarket Management of Cybersecurity in Medical Devices; Draft Guidance for Industry and Food and Drug Administration Staff (draft) 2016

In the EU, the new MDR attempts to address cybersecurity in Section 17 of Annex I.[2]

Other regulations that also address security of medical devices are:

- Directive on Security of Network and Information Systems 2016
- General Data Protection Regulation (GDPR) 2016/679

Tasks of medical writers

So what is the role of the medical writer in all of this? As medical writers, it is our responsibility to protect patient data in the documents we write through appropriate anonymisation techniques. Looking at the above mentioned threats through medical devices, patient anonymisation takes a whole new meaning – it does not only protect patient privacy, it saves lives. In the absence of concrete guidance on the implementation of transparency as required by the MDR, I would like to follow the lead of EMA Policy 0070[1] on CT disclosure and make the following suggested do's and don'ts when writing about medical devices:

- *Avoid using direct identifiers (IDs)*. Direct IDs are information that are directly attributable to a specific individual. Examples would be names, initials, addresses, phone numbers, social security numbers, etc. In clinical data, direct IDs, with the exception of patient study ID, have no scientific utility[1] and need not be in the documents that we write. This may seem obvious to those who are aware of data protection legislations in Europe. However, in other parts of the world, data protection legislations are less stringent. I would like to cite the following example: The abstracts and case reports presented at the Annual Cardiovascular Summit TCTAP are later on published in the Journal of American College of Cardiology. Many of these abstracts start with a patient ID, which could be numbers, but also initials or even names (see a sample abstract TCTAP C-042).[10]
- *Mask, aggregate, or generalise quasi-IDs,* attributes that can indirectly identify individuals. Unlike direct IDs, quasi-IDs do provide important data. Examples are sex, race, birth dates, clinic visit dates, geographic location, or socio-economic information. If possible, only those quasi-IDs (e.g. age group, gender, maybe race or ethnicity) that have scientific utility should be included in a case report or narrative. Relative study dates should be used in lieu of calendar dates. EMA Policy 0070 recommends techniques like masking, generalisation, or aggregation of quasi-IDs to avoid patient re-identification.[1]
- *Do not provide specific medical device information* such as serial numbers and device identifiers. To improve device traceability, the MDR requires Unique Device Identification (UDI) numbers.[2] While traceability enables tracking the safety of each individual device, the specificity that UDI presents also increases the risk of patient re-identification several fold. The routine use of the medical device trade name and model is also to be questioned. Whereas journals and regulatory agencies specify that the generic name or the recommended International Non-Proprietary Name (rINN) of a drug be used in publications and regulatory documents, the nomenclature of medical devices are unclear. In fact, if one looks at publications in biomedical journals, it is common practice to use the proprietary names of devices, followed by the name and location of the manufacturer (example: Medtronic iPro2 blinded CGM system using an Enlite sensor [Medtronic, Northridge, CA]).
- *Finally, practice proactive anonymisation*. This entails using appropriate anonymisation techniques as one writes, with the goal of producing a document that provides optimal privacy protection and requires minimum redaction. Only then can we ensure that the scientific utility of our document is maintained even after disclosure.

Conclusions

Many medical devices are life-saving instruments that patients cannot do without. Despite the threats discussed in this article, the benefits of using these devices far outweigh the risks involved. As medical writers, our task is to reduce risks to privacy and safety as much as possible, but at the same time produce scientifically sound documents that will enable regulators to assess the safety and performance of these devices.

As a reminder of our responsibilities as medical writers, I would like to quote the EMA Policy 0070: "what [we] ultimately want to achieve is to retain a maximum of scientifically useful information on medicinal products for the benefit of the public while achieving adequate anonymisation."[1] ■

References

1. EMA Policy 0070 External guidance on the implementation of the European Medicines Agency policy on the publication of clinical data for medicinal products for human use. 02 Mar 2016; 16 Dec 2016; 12 Apr 2017.
2. European Medicines Agency Clinical Data. https://clinicaldata.ema.europa.eu/.
3. Medical Device Regulation (EU) 2017/… of the European Parliament and of the Council of Europe on medical devices (draft 22 Feb 2017). Available from: http://data.consilium.europa.eu/doc/document/ST-10729-2016-INIT/en/pdf. [Accessed 02 Mar 2017].
4. El Emam K, Jonker E, Arbuckle L, Malin B. A systematic review of re-identification attacks on health data. PLoS One. 2011;6(12):e28071.
5. Reisinger D. How a pacemaker led police to accuse someone with arson. Fortune 07 Feb 2017 Available from: http://fortune.com/ 2017/02/07/pacemaker-arson-charges/. [Accessed 02 Mar 2017].
6. El-Laboudi AH, Misra S, Martineau M, Deol P, Sanders A, Oliver N. Intentional large insulin overdose captured on a continuous glucose monitor: a novel case report. J Diabetes Sci Technol. 2015 Jul;9(4):929-31.
7. Burns AJ, Johnson ME, Honeyman P. A brief chronology of medical device security. Communications of the ACM 2016 Oct;59(10): 66-72.
8. US FDA Safety Communications. Cybersecurity vulnerabilities identified in St. Jude Medical's implantable cardiac devices and Merlin@home transmitter. Available from: https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm. [Accessed 02 Mar 2017].
9. It's insanely easy to hack hospital equipment. Wired 25 April 2014. Available from: https://www.wired.com/2014/04/hospital-equipment-vulnerable/. [Accessed 02 Mar 2017].
10. Chiang L. Provisional strategy rocks? One or two stents. TCTAP C-042. J Am Coll Cardiol – 2014 Apr 01;63(12):S91-S92. Also available from https://www.deepdyve.com/lp/elsevier/tctap-c-042-provisional-strategy-rocks-one-or-two-stents-oYxJsrgXHm. [Accessed 02 Mar 2017].

Conflicts of Interest and Disclaimers

Raquel is an employee of Clinipace Worldwide. The views and opinions in this article are those of author alone and do not necessarily reflect those of her employer.

Author information

Raquel Billiones is a Senior Director for Medical & Regulatory Writing at Clinipace Worldwide. She is based in Zurich where she heads Clinipace's Swiss subsidiary. She has been writing regulatory documents for >11 years, is a long-time EMWA member, MEW section editor of GYFD, and EMWA workshop leader.