GUTcert Interview

## Digital health applications and information security

In October 2021, GUTcert employee Bozena Jakubowska conducted an interview on the topic of ISMS in the medical sector with Ulrich Wegener, auditor at Berlin Cert and scientist in the field of medical technology, following a conference.

The last few years have been very significant for the medical sector. Not only the consequences of the Covid pandemic, but also or above all the automation of almost all processes and the increasing share of artificial intelligence in all areas contributed to this.

During the Medical Devices Day at the Johner Institute, Prof. Dr. Christian Johner announced that with advancing technology development, formal requirements will also increase - which will lead to many small and medium-sized companies having to look for ways to reduce costs. It is likely that almost 50% of companies will have to reduce their own product range because the legal introduction and further development of new products is simply too expensive. This, however, would be fatal and a step in the wrong direction, as innovative solutions are constantly required, especially in the field of medicine.

One of the legal requirements relates to data security and data protection of digital health applications (DiGA): All companies dealing with digital health applications must have an ISMS certificate from 1 January 2022.

Ulrich Wegener, auditor at Berlin Cert and himself working in the medical sector for years, shed light on the subject in a conversation with our staff member Bózena Jakubowska: He explained what really needs to be adapted and how to prepare for ISMS certification as painlessly as possible.

**GC:** At the conference we learned about many aspects of the medical business. How do you assess the situation of the industry?

**Wegener**: Due to the introduction of the Medical Device Regulation (MDR), the industry is still very busy either adapting its technical documentation for the new requirements or taking products off the market. But especially small companies that are new to the market together with the MDR can implement the new requirements without bias.

**GC:** The Digital Health Applications Regulation is a fact. What would you recommend to manufacturers of digital medical products? What challenges do you see and how can one deal with it "smartly"? Does the law leave some freedom of interpretation?

**Wegener**: The ordinance gives quite clear instructions on what has to be implemented and how in order for a DiGA to be recognised as such and for reimbursement to flow from the payers. In particular, the self-declaration according to Annex I of the Ordinance should be mentioned here. The fast-track procedure according to § 139e SGB V offers manufacturers of digital health applications a transparent possibility to bring their product to market quickly.

Your contact person:
Bozena Jakubowska
bozena.jakubowska@gut-cert.de
+49 30 2332021-65

GUTcert
AFNOR Group
GUT Certification Company for
Management Systems mbH
Environmental verifier
Eichenstraße 3 b, 12435 Berlin

**GC:** What can serve as a basis for implementing an information security management system (ISMS)? What are the differences between the systems, and which would you recommend?

**Wegener**: According to point 1 of the basic requirements, which apply to all digital health applications, the manufacturer must answer the question of whether it has implemented an information security management system in accordance with the ISO/IEC 27000 series, BSI standard 200-2 or a comparable system and whether it can present a corresponding recognised certificate or comparable proof at the request of the Federal Institute for Drugs and Medical Devices.

The manufacturer is therefore free to choose the system. I would recommend a system from the ISO/IEC 27000 series because it is leaner than others: The "question catalogue" is smaller and can be adapted to one's own company. Like EN ISO 13485, ISO/IEC 27001 is organised according to the High-Level Structure and, together with EN ISO 27799, can offer a good supplement specifically for healthcare applications.

**GC:** According to this, the introduction of an ISMS should be a little easier for companies that already hold an ISO 13485 certificate. Is there anything you should pay particular attention to?

**Wegener**: As a manufacturer of a medical device, you are familiar with EN ISO 13485, so what could be more obvious than creating an integrated management system and linking ISO/IEC 27001 to the quality management manual (QMH) of EN ISO 13485? It is important to mention that ISO/IEC 27001 does not have a QMH. Important points here are the risk analysis, /which, however, should not scare anyone who has mastered EN ISO 14971, and the "declaration of applicability", i.e. the proof by which measures the protection of values against certain threats is achieved.  This declaration is the basis of the certificate.

**GC:** What approach would you recommend to a manufacturer? And how long does it take to implement an ISMS?

**Wegener**: If you have the idea of developing a DiGA and have not yet had any contact with EN ISO 13485, then you should first deal with ISO/IEC 27001 to get a feel for the standard: It is relatively light fare.

EN ISO 13485 brings with it a whole bouquet of other standards, even if one supposedly only concentrates on the development of a DiGA. However, with the "view through the glasses" of ISO/IEC 27001, it is relatively easy to integrate its aspects into the processes to be described in EN ISO 13485. In doing so, one will notice how small the focus is that EN ISO 13485 places on IT security itself. A side effect could also be that one realises how easy it is to grasp all aspects

Of the DSGVO with an ISMS.

The ISO/IEC 27001 is for me the management system for the GDPR.

You asked about the duration of the introduction: Well, with a small company you are through in a few months, consolidated structures unfortunately need more time, e.g. for the realistic analysis of the actual state as a basis for the risk assessment.

Your contact person:
Bozena Jakubowska
bozena.jakubowska@gut-cert.de
+49 30 2332021-65

GUTcert
AFNOR Group

GUT Certification Company for
Management Systems mbH
Environmental verifier
Eichenstraße 3 b, 12435 Berlin

GUTcert Interview

**GC:** Do you know of any other tools that might be helpful in implementing an ISMS in the medical industry?

**Wegener**: We have currently developed a checklist that anyone interested can use to check whether the established ISMS meets the minimum requirements for a system according to ISO/IEC 27001. However, the checklist cannot replace a risk analysis, but we will soon be able to provide further information in a guide.

**GC:** What feedback do you get from the companies?

**Wegener**: The introduction of another management system is often initially perceived as a burden. But when the idea of an integrated system catches on, the advantages come to the fore. Once the value of a management system for the requirements of the GDPR is recognised, the dam is breached. So far, the feedback has always been positive.

**GC:** What role does the certification industry play for you?

**Wegener**: The Digital Health Applications are starting at a time when the industry is groaning under the introduction of the MDR - there is already a backlog of notified bodies for the MDR. In addition, there is now an additional demand for accredited bodies for ISO/IEC 27001 and further certifications in the area of IT security will come in the near future.

Thus, it is unfortunately foreseeable that medical devices will often not be available at the time they are needed for humans. Here, the certification industry cannot be blamed, because an upsurge is not created as quickly as a fast tack of a DiGA.

**WE WANT TO GET BETTER TOGETHER.**

**Ulrich Wegener**
Auditor ISO13485:2016, scientist in the field of medical technology

**Bozena Jakubowska**
Product Manager ISMS, GUTcert

Your contact person:
Bozena Jakubowska
bozena.jakubowska@gut-cert.de
+49 30 2332021-65

GUTcert
AFNOR Group
GUT Certification Company for
Management Systems mbH
Environmental verifier
Eichenstraße 3 b, 12435 Berlin