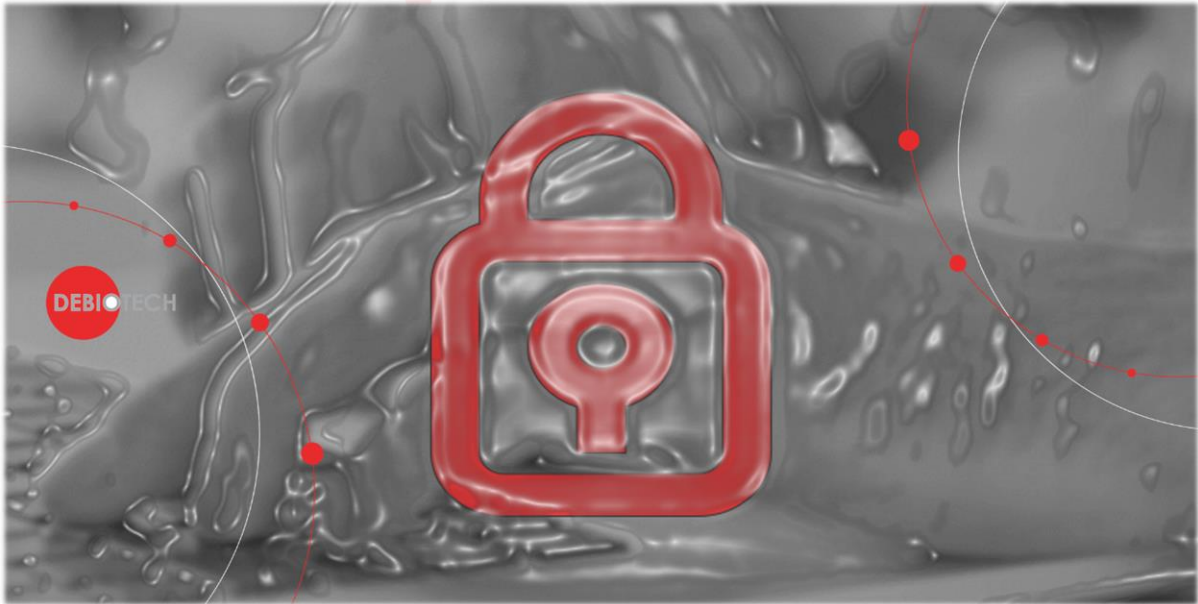


What is Cybersecurity?



1. Goal of this publication


The goal of this publication is to give you a short introduction to a critically important topic for medical devices: Cybersecurity. It gathers high level information critically important for any manufacturer of connected devices.

2. Targeted audience

The information gathered in this publication should be particularly useful for:

- CEO, CTO and C-Level executives
- Head of Software Development Team,
- Software Project Managers,
- DevOps team,
- Software developers.

3. Table of content



1. Goal of this publication	1
2. Targeted audience	1
3. Table of content	2
4. Definitions	3
5. Thoughts and recommendations	4
5.1. Data protection	4
5.2. Data privacy	5
5.3. Data security / Cybersecurity	5
6. Regulatory landscape	6
7. Authors.....	7
8. Next steps	8



4. Definitions

Data protection is the process of safeguarding important information from corruption, compromise or loss and providing the capability to restore the data to a functional state should something happen to render the data inaccessible or unusable.

Data privacy concerns the proper handling of sensitive data including, notably, personal data but also other confidential data, such as health-related data, to meet regulatory requirements as well as protecting the confidentiality and immutability of the data.

Data security (Cybersecurity) is the practice of protecting critical systems and sensitive information from digital attacks throughout its entire lifecycle. Also known as information technology (IT) security, cybersecurity measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization.

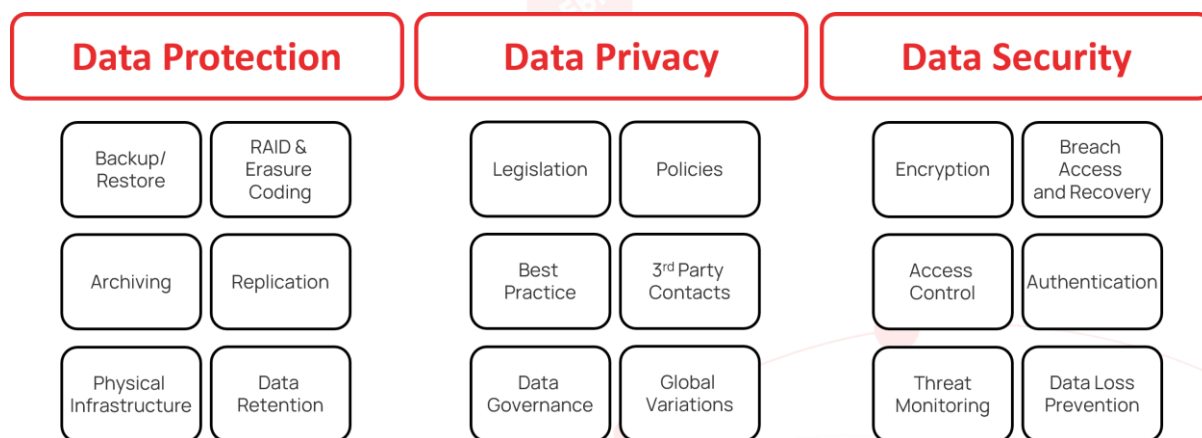


Figure 1. Illustration of content of Data Protection, Security & Privacy

5. Thoughts and recommendations

5.1. Data protection

Data protection has been well understood by a large majority of people. Even non-technical persons are aware that there is a risk to lose all their data if they only rely on a single local copy of those. Who doesn't make backups either in the cloud or on multiple hardware of their precious digital pictures? Various data protection frameworks can be elaborated, and their complexity varies also depending on the risk the data owner perceives.

For MedTech companies, Debiotech recommends to

- Write down your Data Protection Policy: a 1-page document that forces you to describe your high-level strategy and the person responsible for its development within your organization.
- Avoid multiple local copies: the synchronization of those copies will be a burden for any organization.
- Avoid the use of standard cloud services without control on the data localization and ownership: for health-related data, data privacy national regulations might forbid you to do so.
- Have a 3-layer backup strategy with 1 copy on your local server, one copy on a server known to be in a different city but the same country (to ensure national regulations consistency between your backups) and finally, if possible, on a third server with the same constraints (different city but same country). Your data are highly critical, the cost of having a 3-layer backup is balanced by the security you have to retrieve your data in any case. Depending on your country geographical and geopolitical associated risks (for example earthquakes or wars), you might consider having one or two backups in a foreign country with similar data privacy regulation but lower geographical and geopolitical risks.
- Ideally, if you use services of another company to store some of your backups, ensure this company is registered within the same country. This way no foreign law potentially threatening your data privacy can apply to them.

5.2. Data privacy

Data privacy starts to be a mainstream topic. Who hasn't heard about large companies trying to get ownership over the data they store for you through multiple updates of lengthy General Terms and Conditions that no one is reading entirely? There is no single definition about what should be private within your data. National legislations vary a lot on this topic and will apply to your company as soon as you want to enter those countries with your product or even just with prototypes.

For MedTech companies, Debiotech recommends to:

- Write down your Data Privacy Policy: a 1-page document that forces you to describe what you consider as private, and protect accordingly, in the data you collect and the person responsible for its application within your organization.
- Make the distinction between the data you collect through your Human Resources Department and the health-related data that your connected devices are collecting.
- Inform your employees and collaborators that in case of data privacy breach they must report it to the person responsible of the application of your data privacy policy.
- Support the person responsible of the application of your data privacy policy in the development of reusable and validated tools to anonymize data and remove them from your multiple backup copies.

5.3. Data security / Cybersecurity

Data security is still misunderstood by many persons even by managers and entrepreneurs active in Medical Device or even worst in Digital Health. Access control and authentication are usually understood principles but threats and common vulnerabilities assessment or source code analysis are usually more obscure. The execution of those concepts can also have multiple levels of complexity. It is common that they are perceived as burden slowing down your development, however they are critical for the control you have on the safety and security of the data you collect or use. The higher number of actors have access to critical data, the higher the chance that one of them will be subject to a cyberattack and will provide an entry door to those data to digital attackers.

For MedTech companies, Debiotech recommends to:

- Write down your Data Security Policy: a 1-page document that forces you to describe your level of concern about data security and the resources you make available for its management.
- Differentiate your expectations in terms of data security for your own IT-infrastructure and for your products.
- Don't look for shortcuts in the execution of data security, those shortcuts will create entry opportunities for potential intruders.
- Dig further into this topic with our complementary publications

6. Regulatory landscape

Regulatory speaking, data protection and data privacy are usually treated in the same texts. Data security on its side has its own legislations. The applicable regulations usually depend on the type of data: health-related data are usually associated with stronger requirements in term of privacy and security.

Data protection & privacy:

- Europe: GDPR (Europe),
- Switzerland: Federal Act on Data Protection,
- US: HIPAA and numerous data protection laws enacted on both the federal and state levels.

Data security:

- US: HIPAA
- International:
 - UL-2900
 - ISO 27000 Series
 - NIST Cybersecurity Framework

7. Authors

This publication has been written and reviewed by:



Rémi Charrier
Business Development Director
r.charrier@debiotech.com

João Budzinski
R&D Director
j.budzinski@debiotech.com



Laurent Colloud
Software Project Manager
l.colloud@debiotech.com

Gilles Forconi
Software Quality Manager
g.forconi@debiotech.com



Valentin Fischer
IT manager
v.fischer@debiotech.com

8. Next steps

Debiotech is glad to have the opportunity to share its knowledge with innovative companies from the MedTech industry. Your feedbacks on this publication are welcome and will be used to update it or to create new publications on topics you care about.

Continue your education on medical device development by:

- Accessing Debiotech historic publications: <https://www.debiotech.com/news-grid/>
- Following Debiotech on LinkedIn to be notified on new publications: <https://www.linkedin.com/company/debiotech-sa>
- Contacting us to ask a question or request personalized support: contact@debiotech.com

Debiotech would be proud to be your partner and support you with:

- Medical device design & development services:
 - Software: Digital Health, Firmware, Embedded, SaMD
 - Electronics: Design, Verification and Validation
 - Mechanics: Design for micro-fabrication & fluidics systems
 - Supply chain development and optimization
- Support in medical innovation management:
 - Market analysis and segmentation
 - IP management
 - Business plan consolidation
 - Partnership development

