The intended goal of security solutions built around implantable (IMD) medical devices is to protect patient's sensitive data and the device's resources (Rathore et al., 2017). The following security properties should be what implantable medical devices should aim to inherently feature:

Security Feature	Intended Goal	Technology Solution
Confidentiality.	The information exchanged with the IMD should be concealed from unauthorised access.	Cryptography protects data from unauthorised access and disclosure(O'Reilly Media, 2021).
Integrity	To protect the data processed by the IMD and exchanged with the IMD, a more robust authentication mechanism that protects the data from illegal alteration is required	Through the usage of hashing algorithms and message digest, cryptography ensures the integrity and accuracy of information (O'Reilly Media, 2021)
Availability	The objective of implanting a medical device in the body is to provide vital functions that the body has lost the ability to perform. Thus, the device must be available for remote access of the patient to the doctor. The doctor should have access to perform required operations when required.	Authentication is a technique used to authenticate a claimed identity. Authentication ensures that the data or system is accessible to the authenticate subjects. Nonetheless, authentication alone is insufficient to control authenticated subjects ability to modify data or systems without being authorised to do so. Authorisation as an additional layer of protection determines the subject's privileges on accessing the object (Martin, 2019).
Accountability	Nonrepudiation is the assurance that every transaction can be proven to have been performed by a specific subject on a particular object. A party to a contract or communication cannot repudiate the authenticity of their signature on a document or send a message that they originated.	On the internet, a digital signature is a mechanism used not only to ensure that a message or document has been electronically signed by the person that purported to sign the document but also, since a digital signature can only be created by one person, to ensure that a person cannot later deny that they furnished the signature (TechTarget, 2008).

References:

Martin, J. A. (2019) *What is access control? A key component of data security | CSO Online*. Available at: https://www.csoonline.com/article/3251714/what-is-access-control-a-key-component-of-data-security.html (Accessed: 26 May 2021).

O'Reilly Media (2021) *The Role of Cryptography in Information Security - CISSP For Dummies, 4th Edition [Book]*. Available at: https://www.oreilly.com/library/view/cissp-for-dummies/9781118417102/a2_13_9781118362396-ch08.html (Accessed: 25 May 2021).

Rathore, H. et al. (2017) 'A review of security challenges, attacks and resolutions for wireless medical devices', *2017 13th International Wireless Communications and Mobile Computing Conference, IWCMC 2017*, (June), pp. 1495–1501. doi: 10.1109/IWCMC.2017.7986505.

TechTarget (2008) *What is nonrepudiation? - Definition from WhatIs.com*. Available at: https://searchsecurity.techtarget.com/definition/nonrepudiation (Accessed: 26 May 2021).