Initial Post

Case Study: Medical Implants

The ACM Code of Ethics and Professional Conduct applies directly to the case study on medical implants, emphasising ethical principles like "Avoid harm," "Be honest and trustworthy," and "Respect privacy" (ACM, 2024). In the context of medical implants, developers must ensure the devices are safe, reliable, and secure from cyber threats, as failure could lead to severe harm or even loss of life. This aligns with legal obligations such as The regulation of medical devices in great britain, which enforce stringent testing, transparency, and data security standards (Gov.uk, 2021).

The British Computer Society (BCS) Code of Conduct similarly emphasises public interest, integrity, and competence, which are essential when developing medical implants. The BCS stresses the importance of "ensuring that relevant parties are informed of any potential risks" and "ensuring quality of work," which aligns closely with ACM’s ethical mandates (BCS, 2024). Both codes advocate for thorough risk assessments and transparent communication with stakeholders, especially when users' health and privacy are at risk.

The social implications also require attention; for example, any bias in AI algorithms within implants could lead to unequal health outcomes, challenging the ethics of fairness and non-discrimination emphasized by both ACM and BCS codes (Floridi & Taddeo, 2016). Ethical compliance strengthens the professionalism of computing professionals, builds public trust, and ensures legal accountability.

References:

Case study: medical Implants, ACM. (2024). ACM Code of Ethics and Professional Conduct. https://www.acm.org/code-of-ethics/case-studies

Code of conduct BCS. (2024). BCS Code of Conduct. https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct

Gov.uk. (2021). The regulations and how we enforce them. Journal of Medical devices. https://www.gov.uk/government/publications/report-a-non-compliant-medical-device-enforcement-process/how-mhra-ensures-the-safety-and-quality-of-medical-devices

Floridi, L., & Taddeo, M. (2016). What is data ethics? Philosophical Transactions of the Royal Society A. https://royalsocietypublishing.org/doi/full/10.1098/rsta.2016.0360

Response

Hello Mohammed,  
  
Thank you for bringing another insight to the medical implant’s technology case by emphasizing the importance of cybersecurity of medical implant device and the failure to comply with the measures could lead to severe harm or even loss of life. Also, the reference to the legal obligations such as enforcement of stringent testing, transparency, and data security standards as guided by the regulation of medical devices in Great Britain (Gov.uk, 2021) is on point. Addition to the point on cybersecurity of the device, the risks associated with cybersecurity threats and vulnerabilities should be considered throughout all stages in the life of a medical device, from development through end of support (EOS) and there should be cybersecurity risk management in place (International Medical Devic Regulator Forum,2023). Corazon complied with this best practice by having an open bug bounty program inviting disclosure of potential vulnerabilities in their app (Association for Computing Machinery).  
  
Furthermore, the implant medical technology is an example of Healthcare Internet of Things (IoT)devices, and the device do collects and stores sensitive patient information which any vulnerabilities in the device may lead to data breaches, exposing health records, personal information, and medical histories to an unauthorized individual. This challenge could result to legal and privacy-related repercussions as it contravenes GDPR policy and could attracts penalties (Rashid.M, et. al ,2024).  
  
Conclusion  
Compliance by the rules and laws guiding any ethical codes and professional conduct has a long-term benefit to any organisation such as continuity in business, avoiding any penalties or reputational risk and minimization of vulnerabilities of any kind.  
  
Thank you.  
Njide  
  
Reference:  
Association for Computing Machinery (2018) ACM Code of Ethics and Professional Conduct. Available from: https://ethics.acm.org/ [Accessed: 28 August 2024].  
  
Association for Computing Machinery (N.D.) Case: Medical Implant Risk Analysis. Available from: https://ethics.acm.org/code-of-ethics/using-the-code/case-malware-disruption/ [Accessed: 28 August 2024].  
  
International Medical Devic Regulator Forum (2023).Principles and Practices for the Cybersecurity of Legacy Medical Devices. Available from: https://www.imdrf.org/documents/principles-and-practices-cybersecurity-legacy-medical-devices [Accessed 3rd September 2024].  
  
Rashid.M, et, al (2024). European Journal of Electrical Engineering &Computer Science. IoT Complexity: Security, Vulnerabilities and Risks. Vol.8 No. 1. Available from: https://www.ejece.org/index.php/ejece/article/view/597 [Accessed 3rd September 2024)  
  
British Computer Society (BCS), 2022. BCS Code of Conduct. Available from: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/ [Accessed 28 August 2024].

Summary Post

Summary Post: Medical Implants

The development and deployment of medical implants, which are part of the Healthcare Internet of Things (IoT), must adhere to ethical guidelines such as the ACM Code of Ethics and Professional Conduct and the BCS Code of Conduct. These codes emphasise principles like "Avoid harm," "Be honest and trustworthy," "Respect privacy," and "Ensure quality of work" (ACM.2024). Adhering to these ethical mandates is crucial to prevent severe harm or loss of life caused by unsafe or insecure devices. Regulatory frameworks like the UK's regulation of medical devices reinforce these requirements by mandating stringent testing, transparency, and robust data security standards (Gov.uk, 2021).

Feedback from Njideka highlights the critical importance of cybersecurity throughout the entire lifecycle of medical devices—from development to end-of-support (EOS). Effective cybersecurity risk management strategies, such as open bug bounty programs, help identify and mitigate vulnerabilities in medical devices (International Medical Device Regulators Forum, 2023). The case of Corazon demonstrates adherence to best practices by proactively managing potential cybersecurity risks through community engagement (Association for Computing Machinery).

Moreover, medical implants often collect sensitive patient information, and vulnerabilities could result in data breaches that expose personal health records, violating GDPR guidelines and leading to legal and privacy issues (Rashid et al., 2024). Thus, a comprehensive approach that integrates ethical principles, legal obligations, and continuous risk management is essential for medical implant technology. This approach not only builds public trust but also protects patients, ensures compliance, and reduces potential reputational and legal risks for developers and organizations involved in this critical field.

References

Association for Computing Machinery (2018) ACM Code of Ethics and Professional Conduct. Available from: https://ethics.acm.org/ [Accessed: 28 August 2024].

Rashid.M, et, al (2024). European Journal of Electrical Engineering &Computer Science. IoT Complexity: Security, Vulnerabilities and Risks. Vol.8 No. 1. Available from: https://www.ejece.org/index.php/ejece/article/view/597 [Accessed 3rd September 2024)

International Medical Devic Regulator Forum (2023).Principles and Practices for the Cybersecurity of Legacy Medical Devices. Available from: https://www.imdrf.org/documents/principles-and-practices-cybersecurity-legacy-medical-devices [Accessed 3rd September 2024].

Case study: medical Implants, ACM. (2024). ACM Code of Ethics and Professional Conduct. https://www.acm.org/code-of-ethics/case-studies

Code of conduct BCS. (2024). BCS Code of Conduct. https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct

Gov.uk. (2021). The regulations and how we enforce them. Journal of Medical devices. https://www.gov.uk/government/publications/report-a-non-compliant-medical-device-enforcement-process/how-mhra-ensures-the-safety-and-quality-of-medical-devices