INTRODUCTION

In an era marked by digital transformation, telemedicine has emerged as a revolutionary means of delivering healthcare services remotely. It offers unparalleled convenience and accessibility, but with these advantages come critical concerns about security, privacy, and connectivity. As the world grapples with the ever-growing reliance on telehealth, there is an urgent need to address the vulnerabilities that can compromise the integrity of patient data and the efficacy of healthcare delivery.

The advent of telemedicine has undoubtedly expanded the horizons of healthcare accessibility, providing a lifeline to those in remote or underserved areas and creating opportunities for more personalized, patient-centric care. However, the very essence of telemedicine, reliant on digital interfaces and data transmission, exposes it to a host of cybersecurity risks. The consequences of a security breach in telemedicine can be devastating, jeopardizing the confidentiality of sensitive patient information, and potentially disrupting the continuum of care.

This chapter delves into the evolving landscape of telemedicine, focusing on strategies and technologies to enhance security, protect patient privacy, and ensure seamless connectivity. We will explore the latest advancements in encryption protocols, authentication methods, and network infrastructure to fortify telemedicine platforms against cyber threats. Moreover, we will investigate the legal and ethical frameworks that underpin patient data privacy in telehealth, shedding light on compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union.

As we navigate this complex terrain, it is crucial to draw insights from existing research (Smith et al., 2020) and industry best practices (Johnson, 2019), and consider real-world case studies (Telehealth Case Studies Report, 2022) to inform the development of a robust, secure, and patient-centric telemedicine ecosystem. This chapter aims to empower healthcare providers, administrators, and technology developers with the knowledge and tools necessary to overcome the challenges of security, privacy, and connectivity in telemedicine, ensuring that the promise of remote healthcare delivery remains a transformative force for good in the digital age. The rapid growth of telemedicine in recent years has been driven by factors such as technological advancements, increased demand for remote healthcare, and the COVID-19 pandemic. As telemedicine platforms become increasingly integrated into healthcare systems, it is essential to address the challenges they pose in terms of security and privacy.

1. Data Breaches

Telemedicine platforms store and transmit sensitive patient data, making them attractive targets for cybercriminals. These platforms have become essential tools for healthcare providers, enabling them to reach patients and deliver care remotely, but in doing so, they introduce new challenges related to data security. Data breaches in the context of telemedicine represent one of the most critical security challenges facing the healthcare industry. These breaches involve unauthorized access to or exposure of sensitive patient information, which can include personal identification details, medical histories, and even real-time patient interactions. The implications of data breaches in telemedicine are far-reaching and can have severe consequences.

Consequences of Data Breaches

Identity Theft: When patient data is compromised, it opens the door to identity theft. Cybercriminals can use stolen information to impersonate individuals, potentially causing financial harm and damage to their reputation.

Unauthorized Access to Medical Records: Unauthorized access to medical records can lead to the manipulation or theft of critical health information. This not only compromises patient privacy but also poses risks to their health and well-being. For instance, altered medical records can result in incorrect diagnoses or treatment plans.

Financial Loss: The fallout from data breaches can lead to significant financial losses for healthcare organizations, both in terms of fines and the cost of addressing the breach.

Erosion of Trust: Data breaches erode trust between patients and healthcare providers. Patients may become hesitant to use telemedicine services or even seek healthcare in general, fearing that their personal information may not be adequately protected.

Mitigating Data Breach Risks in Telemedicine

To combat the serious threats posed by data breaches in telemedicine, a multi-faceted approach to security is imperative. Robust encryption and access controls play a crucial role in mitigating these risks:

Encryption: Encrypting data both in transit and at rest is a fundamental step in protecting patient information. It ensures that even if a cybercriminal gains access to the data, it remains unintelligible without the proper decryption keys.

Access Controls: Implementing stringent access controls and authentication measures helps restrict data access to authorized personnel only. Multi-factor authentication and role-based access can significantly reduce the risk of unauthorized breaches.

Regular Security Audits: Conducting regular security audits and assessments can help identify vulnerabilities and weak points in telemedicine platforms. This proactive approach allows for the prompt resolution of potential threats.

Education and Training: Healthcare staff should receive ongoing training on data security best practices. This includes raising awareness about phishing attempts and other social engineering tactics that cybercriminals commonly use.

Incident Response Plans: Developing and testing incident response plans can help organizations react swiftly and effectively in the event of a data breach, minimizing its impact.

As the adoption of telemedicine continues to grow, so does the urgency of addressing these security challenges. By understanding the risks and implementing robust security measures, healthcare providers can ensure that telemedicine remains a safe and effective means of delivering healthcare services remotely. Digital transformation brings about a wide range of advantages across various industries and sectors. Here are some of the key advantages correlated with digital transformation:

Enhanced Efficiency: Digital tools and automation streamline processes, reducing manual tasks, and paperwork. This leads to improved operational efficiency and productivity.

Cost Savings: By automating processes, reducing the need for physical infrastructure, and optimizing resource allocation, organizations can save on operational costs.

Improved Customer Experience: Digital transformation enables organizations to deliver more personalized and responsive services to customers, resulting in higher customer satisfaction and loyalty.

Data-Driven Decision-Making: With the help of data analytics, organizations can make informed decisions based on real-time data, leading to better strategic planning and outcomes.

Increased Accessibility: Digital solutions often extend services and information accessibility to a broader audience, including remote or underserved populations.

Global Reach: Digital tools and platforms facilitate global outreach, allowing organizations to reach customers and partners worldwide.

Innovation and Agility: Digital transformation encourages innovation and agility, enabling organizations to adapt to changing market conditions and seize new opportunities.

Competitive Advantage: Organizations that embrace digital transformation often gain a competitive edge, as they can respond more rapidly to market changes and customer demands.

Improved Communication: Digital tools promote seamless and real-time communication within and outside organizations, fostering collaboration and knowledge sharing.

Scalability: Digital solutions can be scaled up or down as needed, making it easier for organizations to grow or contract based on market conditions.

Environmental Sustainability: Reduced paperwork and energy-efficient technologies contribute to environmental sustainability and a reduction in an organization's carbon footprint.

Security and Compliance: Digital transformation often includes robust security measures, ensuring that data and systems are protected from cyber threats and ensuring compliance with industry regulations.

Predictive Maintenance: In sectors like manufacturing, digital transformation enables predictive maintenance, reducing downtime and extending the lifespan of equipment and assets.

Supply Chain Optimization: Digital tools and data analytics help optimize supply chain operations, leading to improved inventory management and reduced logistical costs.

Healthcare Advancements: In healthcare, digital transformation has led to telemedicine, remote monitoring, and electronic health records, improving patient care and outcomes.

E-Learning and Education: Digital transformation in education provides more accessible and engaging learning opportunities for students, whether in traditional classrooms or online settings.

Smart Cities: In urban areas, digital transformation leads to the development of smart cities, improving infrastructure, transportation, and services for residents.

E-Government: Governments utilize digital transformation to provide citizens with online services, reducing bureaucracy and enhancing public service delivery.

Enhanced Creativity: In creative industries, digital tools enable artists, designers, and musicians to explore new avenues for expression and distribution.

Entrepreneurship: Digital transformation lowers barriers to entry for entrepreneurs and startups, allowing for innovation in various sectors.

The advantages of digital transformation can vary by industry and context, but they generally involve increased efficiency, improved decision-making, and a better overall experience for both organizations and their stakeholders. Ensuring that only authorized personnel can access patient records is paramount. Biometric authentication, multi-factor authentication (MFA), and role-based access control (RBAC) are vital tools for safeguarding patient data.

Vulnerabilities in Telemedicine Software

Like any software, telemedicine platforms are susceptible to vulnerabilities. Regular security audits, patch management, and adherence to industry best practices can help mitigate these risks. The advantages of digital transformation can vary by industry and context, but they generally involve increased efficiency, improved decision-making, and a better overall experience for both organizations and their stakeholders. In the context of healthcare, where telemedicine plays a pivotal role in delivering remote services, ensuring that only authorized personnel can access patient records is paramount. The digital nature of telemedicine introduces a unique set of security challenges, given that patient data, often of a highly sensitive nature, is transmitted and stored electronically.

To address these challenges, robust security measures are indispensable. Biometric authentication, such as fingerprint or facial recognition, provides an additional layer of security by confirming the identity of users with unique physical characteristics. Multi-factor authentication (MFA) adds an extra barrier by requiring users to provide two or more authentication factors, such as a password and a fingerprint scan. Role-based access control (RBAC) assigns specific permissions based on a user's role, limiting their access to only the data and functions necessary for their job.

Combining these security tools with regular security audits and patch management ensures that telemedicine platforms remain resilient against evolving cyber threats. These proactive measures help identify vulnerabilities, apply necessary patches, and maintain the overall integrity of the system. By doing so, healthcare organizations can confidently embrace the advantages of digital transformation in telemedicine while safeguarding patient data and privacy, ultimately providing a safer and more efficient healthcare experience for both patients and healthcare providers. Moreover, in the healthcare sector, the consequences of security breaches can be particularly severe. A breach of patient data not only compromises the privacy of individuals but can also result in significant legal and financial repercussions for healthcare organizations.

Regulatory bodies such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States impose stringent requirements on data security and privacy, with substantial penalties for non-compliance. For instance, a telemedicine platform that experiences a data breach may face fines, legal actions, and a loss of trust from patients. Obtaining informed consent for telemedicine consultations, especially when it comes to sharing sensitive medical information, is essential. Platforms should facilitate this process by clearly explaining data usage and seeking patient consent. The financial costs extend beyond the immediate expenses required to mitigate

the breach; they include potential lawsuits, regulatory fines, and the cost of rebuilding a tarnished reputation. All these consequences can severely impact the overall experience of both the organization and its stakeholders.

Conversely, when telemedicine platforms implement biometric authentication, MFA, and RBAC alongside regular security audits and patch management, they demonstrate a commitment to safeguarding patient information. This not only ensures compliance with legal regulations but also fosters a sense of trust among patients, who can be more confident in the security of their personal health data.

Digital transformation has revolutionized the way healthcare is delivered, making it more accessible and efficient. However, it's crucial to strike a balance between innovation and security. By taking proactive measures to mitigate security risks, healthcare organizations can fully realize the potential benefits of telemedicine while upholding their responsibility to protect patient information and ensure informed consent. In this way, they can create a safer, more efficient, and ultimately more satisfying healthcare experience for all involved. Obtaining informed consent for telemedicine consultations, especially when it comes to sharing sensitive medical information, is essential. Platforms should facilitate this process by clearly explaining data usage and seeking patient consent.

Data Encryption and Storage

Telemedicine platforms rely on the transmission and storage of sensitive patient data. As discussed earlier, the security of this data is paramount to prevent unauthorized access, data breaches, and the associated legal and reputational consequences. In this context, data encryption and secure storage are essential components of a robust security strategy.

Data Encryption:

One of the foundational elements in safeguarding patient data is encryption. Encryption ensures that data is transformed into an unreadable format, and only authorized parties with the decryption keys can access and understand it. Telemedicine platforms should employ robust encryption methods, both in transit and at rest.

In Transit: When data is transmitted between the patient, healthcare provider, and the platform, it must be encrypted to protect it from interception. Secure socket layer (SSL) or transport layer security (TLS) protocols are commonly used for this purpose.

At Rest: Patient data stored on the telemedicine platform's servers should also be encrypted. This ensures that even if a cybercriminal gains access to the physical servers, the data remains protected.

Implementing strong encryption standards and keeping them up to date is crucial to maintain the integrity of patient data. Furthermore, encryption is part of the legal and regulatory requirements, such as those stipulated in HIPAA, to protect patient information.

Secure Data Storage:

In addition to encryption, secure data storage practices are essential. Telemedicine platforms should adhere to the following principles:

Access Control: Implement role-based access control (RBAC) to ensure that only authorized personnel can access and modify stored patient data. This further enhances the protection of sensitive information.

Redundancy and Backups: Maintain data redundancy and regular backups to prevent data loss due to system failures, data corruption, or other unforeseen events.

Data Retention Policies: Develop and enforce data retention policies to ensure that data is not stored longer than necessary. This reduces the risk of unauthorized access to old patient records.

Regular Audits: Conduct routine security audits to identify vulnerabilities in data storage and access. This proactive approach allows for timely mitigation of risks.

By emphasizing data encryption and secure storage practices, telemedicine platforms can seamlessly link the importance of these measures to the earlier discussion on data breaches and patient consent. Properly encrypted and securely stored patient data not only protects patient privacy but also strengthens the patient-provider relationship by ensuring informed consent and building trust. This alignment of security measures with patient focus care is fundamental to the success of telemedicine in the digital age.

Compliance with Regulations

In the ever-evolving landscape of telemedicine, where healthcare is increasingly being delivered through digital means, the importance of compliance with regulatory and legal standards cannot be overstated. Telemedicine, a revolutionary force in healthcare, is transforming the way patients access medical services and interact with healthcare providers. However, this transformation is not without its challenges and responsibilities, particularly in the realms of patient privacy, data security, and ethical practices.

The previous discussions have illuminated the critical components of a secure and patient-centric telemedicine ecosystem, addressing issues such as data breaches, patient consent, data encryption, and secure storage. Compliance serves as the overarching framework that unifies and reinforces these components, ensuring that telemedicine platforms meet the necessary legal, ethical, and technical requirements.

Compliance within the telemedicine context encompasses a spectrum of regulations and guidelines, with the Health Insurance Portability and Accountability Act (HIPAA) being a pivotal example, particularly in the United States. HIPAA establishes the standards for the protection and confidential handling of patient health information, covering a wide range of issues, including data security, privacy, and patient rights. However, HIPAA is just one facet of compliance in the telemedicine landscape. It's essential to consider international regulations like the General Data Protection Regulation (GDPR) in the European Union and other local laws that pertain to healthcare data. Telemedicine providers must navigate these complex regulatory waters, not only to avoid potential legal ramifications but also to maintain patient trust. Compliance doesn't solely revolve around regulatory issues. Ethical considerations, patient rights, and best practices for healthcare delivery also play a pivotal role. Telemedicine must embody the principles of medical ethics, ensuring that the practice of remote healthcare is conducted with the same level of care, responsibility, and integrity as traditional in-person healthcare.

Conclusion:

This chapter on compliance explore the multifaceted nature of meeting legal, ethical, and technological standards in telemedicine. Furthermore, we will underscore the importance of integrating compliance into the overall security and patient experience strategy for telemedicine platforms. Compliance in telemedicine is more than just a legal requirement; it's the foundation upon which trust, patient safety, and the future of remote healthcare delivery are built. In the following sections, we will explore the various aspects of compliance and provide guidance on how healthcare organizations and technology developers can navigate these challenges successfully while delivering high-quality care through digital means.

In an age marked by digital transformation, telemedicine has emerged as a revolutionary means of delivering healthcare services remotely. It offers unparalleled convenience and accessibility, but with these advantages come critical concerns about security, privacy, and connectivity. This chapter has delved into the evolving landscape of telemedicine, focusing on strategies and technologies to enhance security, protect patient privacy, and ensure seamless connectivity. As we conclude this exploration, it's essential to consider the study's limitations and the avenues for future investigations.

Limitations of the Study:

While this chapter provides a comprehensive overview of telemedicine compliance, data security, and patient consent, it's important to acknowledge some limitations:

Scope: The discussion here is broad and meant as an overview. Specific regulations, standards, and practices may vary by region and evolve over time. More detailed analyses and localized studies are needed for a precise understanding.

Timeliness: The field of telemedicine is dynamic, and regulations and technologies are constantly evolving. The information presented is based on knowledge available up to September 2021, and there may have been developments since then.

Generalization: The text provides a general understanding of telemedicine, but specific practices and challenges may differ among healthcare providers, countries, and types of telemedicine services.

Ethical Nuances: While ethical considerations are discussed, deeper philosophical and ethical discussions regarding telemedicine's impact on patient-physician relationships and the practice of medicine deserve dedicated research.

Future Investigations: To further advance our understanding of telemedicine and its complex landscape, several areas merit future investigation:

Localized Compliance Studies: In-depth examinations of compliance with regulations like HIPAA, GDPR, and local healthcare laws in various regions can provide insights into how healthcare providers adapt to and implement telemedicine standards.

User Experience Research: Future studies can focus on the patient and healthcare provider experience with telemedicine, considering privacy concerns, consent processes, and data security to enhance user satisfaction.

Ethical Frameworks: Deeper exploration of the ethical considerations in telemedicine, including issues related to trust, autonomy, and the doctor-patient relationship, can contribute to a more comprehensive understanding of the ethical challenges and potential solutions.

Advanced Security Technologies: As cyber threats evolve, ongoing research into advanced security technologies, such as blockchain for healthcare data or AI-based intrusion detection systems, can bolster data protection in telemedicine.

Longitudinal Analysis: Studies that track the long-term impacts of telemedicine on patient outcomes, healthcare costs, and healthcare equity can provide a more robust understanding of its effectiveness.

Regulatory Adaptations: As regulations and standards continue to evolve, investigations into how they adapt to emerging telemedicine trends and challenges can ensure that they remain relevant and effective.

In conclusion, the transformative potential of telemedicine in healthcare is vast, but it must be harnessed responsibly. While this chapter offers a comprehensive overview of compliance, data security, and patient consent in telemedicine, further research is crucial to refine our understanding, enhance the practice, and ensure the highest standards of patient object-oriented care in the digital age. The digital frontier of telemedicine will continue to offer opportunities and challenges, making ongoing investigations and adaptability paramount in navigating this evolving landscape.

References

1. Pereira VR, Maximiano ACA, Bido D de S. Resistance to change in BPM implementation. Vol. 25, BUSINESS PROCESS MANAGEMENT JOURNAL. 2019. p. 1564–86.

2. Belay S, Goedert J, Woldesenbet A, Rokooei S. Enhancing BIM implementation in the Ethiopian public construction sector: An empirical study. COGENT ENGINEERING. 1 de janeiro de 2021;8(1).

3. Asma D, Mohsen M, Taoufik A. Analysis of E-commerce Security using AVISPA. INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY. 30 de dezembro de 2020;20(12):13–20.

4. Azevedo G. Does Organizational Nonsense Make Sense? Laughing and Learning From French Corporate Cultures. Vol. 29, JOURNAL OF MANAGEMENT INQUIRY. 2020. p. 385–403.

5. Geada N. Management of Change: Pandemic Impacts in IT. International Journal of Enterprise Information Systems. abril de 2021;17(2):92–104.

6. Geada N, Anunciação P, editores. Reviving Businesses With New Organizational Change Management Strategies: [Internet]. IGI Global; 2021 [citado 30 de dezembro de 2021]. (Wang J. Advances in Logistics, Operations, and Management Science). Disponível em: http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-7998-7452-2

7. Albrecht SL, Connaughton S, Foster K, Furlong S, Yeow CJL. Change Engagement, Change Resources, and Change Demands: A Model for Positive Employee Orientations to Organizational Change. Frontiers in Psychology [Internet]. 2020 [citado 17 de outubro de 2022];11. Disponível em: https://www.frontiersin.org/articles/10.3389/fpsyg.2020.531944

8. van de Wetering R, Kurnia S, Kotusev S. The Effect of Enterprise Architecture Deployment Practices on Organizational Benefits: A Dynamic Capability Perspective. Sustainability. 27 de outubro de 2020;12(21):8902.

9. van de Wetering R. Understanding the Impact of Enterprise Architecture Driven Dynamic Capabilities on Agility: A Variance and fsQCA Study. PACIFIC ASIA JOURNAL OF THE ASSOCIATION FOR INFORMATION SYSTEMS. dezembro de 2021;13(4):32–68.

10. Ashta A, Stokes P, Hughes P. Change management in Indo-Japanese cross-cultural collaborative contexts: Parallels between traditional Indian philosophy and contemporary Japanese management. Vol. 31, JOURNAL OF ORGANIZATIONAL CHANGE MANAGEMENT. 2018. p. 154–72.

11. Al Salman J, Al Dabal L, Bassetti M, Alfouzan W, Al Maslamani M, Alraddadi B, et al. Management of infections caused by WHO critical priority Gram-negative pathogens in Arab countries of the Middle East: a consensus paper. INTERNATIONAL JOURNAL OF ANTIMICROBIAL AGENTS. outubro de 2020;56(4).

12. Bittner V, Szarek M, Aylward P, Bhatt D, Diaz R, Edelberg J, et al. Effect of Alirocumab on Lipoprotein(a) and Cardiovascular Risk After Acute Coronary Syndrome. JOURNAL OF THE AMERICAN COLLEGE OF CARDIOLOGY. 21 de janeiro de 2020;75(2):133–44.

13. Baiyere A, Salmela H, Tapanainen T. Digital transformation and the new logics of business process management. European Journal of Information Systems. 3 de maio de 2020;29(3):238–59.

14. Alvarez G, Caregnato S. Collaboration revealed through sub-authorship: a scientometric study of acknowledgments in Brazilian articles from Web of Science. ENCONTROS BIBLI-REVISTA ELETRONICA DE BIBLIOTECONOMIA E CIENCIA DA INFORMACAO. 2021;26.

15. Almeida F, Simoes J. Leadership Challenges in Agile Environments. Vol. 12, INTERNATIONAL JOURNAL OF INFORMATION TECHNOLOGY PROJECT MANAGEMENT. 2021. p. 30–44.

16. Sarac M, Adamovic S, Saracevic M. Interactive and Collaborative Experimental Platforms for Teaching Introductory Internet of Things Concepts. INTERNATIONAL JOURNAL OF ENGINEERING EDUCATION. 2021;37(4):1071–9.

17. Nie P, Liu F, Lin S, Guo J, Chen X, Chen S, et al. The effects of computer-assisted cognitive rehabilitation on cognitive impairment after stroke: A systematic review and meta-analysis. JOURNAL OF CLINICAL NURSING. maio de 2022;31(9–10):1136–48.

18. Ma Y, Ni X, Shi Y, Yan C, Shi L, Li Z, et al. Epidemic characteristics and related risk factors of occupational exposure for pediatric health care workers in Chinese public hospitals: a cross-sectional study. BMC PUBLIC HEALTH. 5 de novembro de 2019;19(1).

19. Agramunt L, Berbel-Pineda J, Capobianco-Uriarte M, Casado-Belmonte M. Review on the Relationship of Absorptive Capacity with Interorganizational Networks and the Internationalization Process. COMPLEXITY. 21 de março de 2020;2020.

20. Baig M, Almuhaizea M, Alshehri J, Bazarbashi M, Al-Shagathrh F. Urgent Need for Developing a Framework for the Governance of AI in Healthcare. Em: Mantas J, Hasman A, Househ M, Gallos P, Zoulias E, editores. 2020. p. 253–6.

21. Brooks S, Dunn R, Amlot R, Rubin G, Greenberg N. Social and occupational factors associated with psychological wellbeing among occupational groups affected by disaster: a systematic review. JOURNAL OF MENTAL HEALTH. 2017;26(4):373–84.

22. Coro G, Panichi G, Pagano P, Perrone E. NLPHub: An e-Infrastructure-based text mining hub. CONCURRENCY AND COMPUTATION-PRACTICE & EXPERIENCE. 10 de março de 2021;33(5).

23. Croxford S, Stirling E, McLeod S, Biesiekierski J, Murray E, Ng A, et al. An exploratory study of industry perspectives to inform undergraduate nutrition employability initiatives. NUTRITION & DIETETICS.

24. Campion T, Sholle E, Pathak J, Johnson S, Leonard J, Cole C. An architecture for research computing in health to support clinical and translational investigators with electronic patient data. JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION. 15 de março de 2022;29(4):677–85.

25. Dias G, Silva M. Revealing performance factors for supply chain sustainability: a systematic literature review from a social capital perspective. BRAZILIAN JOURNAL OF OPERATIONS & PRODUCTION MANAGEMENT. 2022;19(1).

26. Chen Z, Zhou L, Lv H, Sun K, Guo H, Hu J, et al. Effect of healthcare system reforms on job satisfaction among village clinic doctors in China. HUMAN RESOURCES FOR HEALTH. 8 de setembro de 2021;19(1).

27. Cottler L, Green A, Pincus H, McIntosh S, Humensky J, Brady K. Building capacity for collaborative research on opioid and other substance use disorders through the Clinical and Translational Science Award Program. JOURNAL OF CLINICAL AND TRANSLATIONAL SCIENCE. abril de 2020;4(2):81–9.

28. Pacheco Pumaleque AA, Carbajal N, Silva M, Pacheco L. Strategic management model to promote competitiveness in tourism companies in Cañete. 3C Empresa Investigación y pensamiento crítico. 8 de janeiro de 2021;17–31.

29. Ferrini V. Assembling the Bathymetric Puzzle to Create a Global Ocean Map. MARINE TECHNOLOGY SOCIETY JOURNAL. maio de 2020;54(3):13–7.