

Chapter 7


Cybersecurity Leadership Ethics in Healthcare

Jorja B. Wright

 <https://orcid.org/0000-0002-7028-995X>

Capitol Technology University, USA

Darrell Norman Burrell

 <https://orcid.org/0000-0002-4675-9544>

Capitol Technology University, USA & Marymount University, USA & University of North Carolina at Chapel Hill, USA

ABSTRACT

Ethical leadership transforms and unites social systems around common purposes of ethicality leveraging organizational connectedness. Cybersecurity and the ethics around it create a variety of complexities. Often healthcare organizations do not openly disclose the extent and nature of cyber data thefts and breaches, which puts those whose information has been exposed at significant risk. It often is whistleblowing that leads to the public finding out the severity of the attack. This requires the need to understand the importance of ethical organizational cultures and the decision-making process that takes place when medical organizations have cybersecurity breaches. Leadership value systems mitigate subjectivity constituting ethical themes of moral character and virtues to advance organizational trust. Healthcare organizational cybersecurity leaders employ strategic foresight to forge connections with ethicality. Ethical leadership implores professional competence and exemplary service cultivating in social responsibility.

INTRODUCTION

The U.S. Securities and Exchange Commission issued new guidance calling on public companies to be more forthcoming when disclosing nature and scope of cybersecurity breaches. This requires that healthcare organizations create cultures where employees develop ethical leadership skills about the nature, impact, and aspects of a cybersecurity breaches in healthcare organizations (Burrell et al., 2019, 2020, 2021).

DOI: 10.4018/978-1-6684-7207-1.ch007

Constant pressure is placed on leaders to be exemplary in virtue ethics in the face of ethical failure and dilemmas that result in dysfunctional organizational practices and discord among stakeholders (Boekhorst, 2015). Ethicality and connectedness converge dimensions of leadership virtues. Ethical knowledge, skill, and willpower underscore virtuous norms, motivations, and foundations to induce strategic thinking and behavior (Joosten, 2014; Crossan et al., 2013; Maio, 2013; Bruce and Langdon, 2000; & Fehr, Kai Chi, and Dang, 2015). Ethical leaders conveying critical thought to organizational connectedness, encourage stakeholders to be influential in developing moral character through constant engagement, reinforcing policies, and modeling virtuous decisions that achieve organizational aims of ethicality (Crossan et al., 2013). Ethical and honest disclosures after cybersecurity breach is critical to helping those involved respond appropriately to the risks.

A leadership strategy to cultivate communal agreement on ethical policies creates an ethical climate that engages healthcare organizations to align the culture profile norms with organizational values (Joosten, Dijke, Hiel, & Cremer, 2014). Strategic planning is imperative to discipline leaders and stakeholders who require oversight in upholding ethical norms that forge interpersonal skills and resolve critical issues negating morality (Malphurs, 2005). Ethical leaders communicate the organization's mission with a conviction to garner connectedness (Boekhorst, 2015). Connectedness underscores team endeavors to reframe and reshape dysfunctional schemas with knowledge sharing and constancy to exemplify credibility, cultural sensitivity, and prosocial interpersonal skills (Gorjean, Resick, & Dickson, 2004). Ethical foundations set leadership cognitive, emotional, and behavioral patterns (Ciulla, 2004).

The field of healthcare is continuously evolving, and the use of technology has revolutionized the way healthcare is delivered. In recent years, healthcare organizations have become a prime target for cyberattacks (Raghupathi & Raghupathi, 2018). This is because healthcare organizations collect and store vast amounts of sensitive patient information, such as medical records, financial information, and personal identification. As such, healthcare cybersecurity and patient information security have become a top priority for healthcare organizations worldwide (Raghupathi & Raghupathi, 2018). Ethical considerations should also play a role in the development and implementation of healthcare cybersecurity strategies (Raghupathi & Raghupathi, 2018).

THE ETHICAL DECISION-MAKING MODEL PROPOSED BY BEAUCHAMP AND CHILDRESS

Beauchamp and Childress proposed an ethical decision-making model that consists of four principles: respect for autonomy, non-maleficence, beneficence, and justice (Beauchamp & Childress, 2019). These four principles provide a framework for healthcare professionals to make ethical decisions in their practice.

Respect for Autonomy

Respect for autonomy requires healthcare professionals to respect the rights of patients to make their own decisions about their healthcare. In the context of healthcare cybersecurity and patient information security, this principle emphasizes the importance of obtaining informed consent from patients before their data is collected, stored, or used (Beauchamp & Childress, 2019; Raghupathi & Raghupathi, 2018).

Informed consent requires patients to be informed of the risks and benefits of sharing their data and to be given the opportunity to consent or refuse to share their data. Healthcare organizations should pro-

10 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/cybersecurity-leadership-ethics-in-healthcare/321016

Related Content

Building Dynamic Business Process in P2P Semantic Web

Timon C. Duand Eldon Y. Li (2009). *Selected Readings on Information Technology and Business Systems Management* (pp. 186-201).

www.irma-international.org/chapter/building-dynamic-business-process-p2p/28639

A Steady-State Framework for Integrated Business Change and Information Systems Development and Maintenance

Simon McGinnes (2012). *Measuring Organizational Information Systems Success: New Technologies and Practices* (pp. 158-177).

www.irma-international.org/chapter/steady-state-framework-integrated-business/63452

Feral Information Systems and Workarounds: The Present Position

Don Kerr (2014). *Feral Information Systems Development: Managerial Implications* (pp. 23-42).

www.irma-international.org/chapter/feral-information-systems-and-workarounds/94675

Theoretical Foundations of Inter-Organizational Information Systems: Towards a Framework Grounded on Seven Theories

Maria Madlberger (2012). *Inter-Organizational Information Systems and Business Management: Theories for Researchers* (pp. 33-49).

www.irma-international.org/chapter/theoretical-foundations-inter-organizational-information/61604

Technology Institutionalisation through Technological, Organisational, and Environmental Isomorphism

Azadeh Pishdadand Abrar Haider (2015). *Business Technologies in Contemporary Organizations: Adoption, Assimilation, and Institutionalization* (pp. 54-74).

www.irma-international.org/chapter/technology-institutionalisation-through-technological-organisational-and-environmental-isomorphism/120751