**Ethical Analysis of Ransomware Attack on ACME Private Hospital**

Author's Name

Institutional Affiliation

Course Code and Name

Instructor's Name

Due Date

**Ethical Analysis of Ransomware Attack on ACME Private Hospital**

**Introduction**

The emergence of threats from cyberspace puts today's organizations, especially healthcare ones, at unprecedented risk. ACME Private Hospital has recently experienced a ransomware attack that locked patients' medical records, and the Incident created the following ethical dilemma for the senior management team. The team must consider whether they need to give the ransom to reclaim the information or if they have to face the results of lost or changed documents. Each case poses substantial ethical and practical concerns. Therefore, this essay will discuss the ethical issue based on ethical theories and practices such as utilitarianism and deontological ethics and recommend the best solution for the hospital.

**Ethical Dilemma Faced by the Senior Management Team**

The senior management of ACME Private Hospital's main decision is whether to pay the ransom. If they pay the ransom, they could quickly retrieve the hospital's crucial patient data, which is essential for patient treatment, without significant delays (Feldman & Kenney, 2024)). However, paying the ransom means providing financial support for criminals and their actions; it may lead to similar situations in the future and act as a precedent for similar incidents.

On the other hand, not paying the ransom would ensure that the hospital does not interact with cyber criminals, aligning with ethical reasoning. However, such an outcome would be undesirable since it could lead to the inability to access updated patient data, a delay in providing medical assistance, and possible deterioration of patients' health conditions. The ethical issue here pertains more to the immediate benefits of paying the ransom to patients' lives and the potential long-term repercussions on the hospital and society.

**Ethical Analysis First Option: Paying the Ransom**

1. **Utilitarian Approach to Paying the Ransom**

The primary ethical approach that aligns with paying the ransom is practical, which means that an action that causes the most benefits to the majority of people should be taken. From a utilitarian perspective, the direct restoration of patient data contributes the most to general happiness (Baraldi, 2024). The patient will continue to benefit from the get-go from having timely access to their records to receive treatment. Of course, the normal operations of the hospital should commence. Employees and healthcare givers would also be relieved from the stress and complications of handling half-baked data, and medical mishaps would be reduced.

However, utilitarianism also looks at the impact of an action beyond the act itself. Ransom payment is received and spent to continue the criminal activity and develop new ransomware attacks for ACME Hospital and other companies. While regaining the data would help, this has to be less important than the long-term consequences of providing a foundation for the continuation of cybercrimes. The reason is that whenever such entities, including hospitals and other organizations, give in to the demands made by the hackers, ransom attacks are likely to occur more frequently and become more severe, thus posing a higher risk to society.

1. **Deontological (Kantian) Ethics on Paying the Ransom**

Kantian ethics, which believes in duty and moral principles, is against ransom payments. Kant's categorical imperative requires that one only universally do what can be made law (White, 2022). Paying the ransom would not meet this criterion because it entails acting against one's ethical responsibility to combat evil and injustice.

Thus, again, Kant's focus on autonomy and dignity speaks against paying the ransom. By yielding to the criminals, the hospital loses its sovereignty, thereby letting such hackers steer the organization's actions. This undermines the hospital's ethical status and sends a message to would-be criminals that such actions will be paid, which goes against the principle that no organization should be put under pressure to perform an unethical task.

**Ethical Analysis Second Option: Refusing to Pay the Ransom**

1. **Beneficence and Non-maleficence in Refusing the Ransom**

According to the principles of beneficence (doing good) and non-maleficence (not harm) that underpin medical ethics, the child should not be told. Declining to meet the ransom may seem counterintuitive to these principles since inadequate medical information hinders a hospital's capacity to Render adequate healthcare services to patients (Cheraghi et al., 2023). Patients could be harmed if their care is delayed or misdiagnosed due to PR records that are either incomplete or still being awaited, violating the non-maleficence principle.

However, goodwill also applies beyond the present circumstances but in the best interest of the whole. The hospital's decision to forgo the ransom payment makes the attackers see the negative impact of their activities on society, thus preventing them from further engaging in the activity. Abstaining from interacting with criminals is beneficial to creating a safer and less corrupt World Wide Web, in which the hospital is responsible for protecting the interest of its patients and society.

1. **Autonomy and Justice in Refusing the Ransom**

Another essential principle is autonomy; in this case, the hospital can make case decisions without undue influence from other sources. Not paying the ransom helps the hospital remain ethical and gives it sufficient strength not to succumb to criminal coercion. This decision also affects justice, which deals with fairness and equity when preparing for decisions.

This can result in unequal consequences because institutions that have the capital for it can pay the ransom, but those that cannot, namely small organizations or other institutions, are more likely to suffer severe repercussions (Davis & Wilner, 2022). By not paying, ACME Private Hospital ensures fairness in society rather than spending money on criminals to pressure the organizations.

**Critical Discussion: Why Refusing the Ransom is the Better Option**

Having analyzed the two scenarios that might result from paying the ransom, I recommend that ACME Hospital does not release the ransom. Although this decision may lead to temporary patient care disruptions, the latter's ethical ramifications are much more severe than any outcomes of paying the ransom. On the other hand, paying would encourage malicious activity and result in more healthcare organizations being targeted and compromised (Connolly & Borrion, 2022). Not paying complies with autonomy, justice, and beneficence since the hospital does not support such activities and discourages the increased incidence of cybercrimes.

To reduce such consequences in the short term, the hospital can restore data from the backup if it has one or engage cybersecurity professionals to help decrypt the information. Long-term measures that ACME Hospital has to undertake include more frequent data backups, improved employee awareness of the risks they pose, and installing better detection mechanisms (Fenech et al., 2024). These steps will assist in fortifying the hospital's protection against other future attacks while upholding the ethical requirements.

**Conclusion**

Accordingly, ACME Private Hospital faces an extensive ethical dilemma after the ransomware attack. By applying utilitarianism and deontology principles, the best decision is to reject the idea of paying ransom. As for spending, it may help to avoid such problems temporarily but contributes to criminals' actions and creates a precedent. Saying no aligns with autonomy, justice, beneficence, and non-maleficence, thus assisting the hospital in staying up-to-date with moral standards. That is why such a decision will foster an ethical and more secure future for the hospital and society, preserving the significance of the patient's interests and ethical responsibilities for the future.

**References**

Baraldi, F. (2024). Should I Pay, Or Should I Quash? The Role of Governments’ Ideology in Ransom Payment. *Defence and Peace Economics*, 1-20. <https://doi.org/10.1080/10242694.2024.2352674>

Cheraghi, R., Valizadeh, L., Zamanzadeh, V., Hassankhani, H., & Jafarzadeh, A. (2023). Clarification of ethical principle of the beneficence in nursing care: an integrative review. *BMC nursing*, *22*(1), 89. <https://doi.org/10.1186/s12912-023-01246-4>

Connolly, A. Y., & Borrion, H. (2022). Reducing ransomware crime: analysis of victims’ payment decisions. *Computers & Security*, *119*, 102760. <https://doi.org/10.1016/j.cose.2022.102760>

Davis, J., & Wilner, A. (2022). Paying terrorist ransoms: Frayed consensus, uneven outcomes & undue harm. *International Journal*, *77*(2), 356-367.<https://doi.org/10.1177/00207020221130308>

Feldman, M., & Kenney, M. (2024). Private Equity and the Demise of the Local: The Loss of Community Economic Power and Autonomy. *Elements in Reinventing Capitalism*. <https://doi.org/10.1017/9781009321853>

Fenech, J., Richards, D., & Formosa, P. (2024). Ethical principles shaping values-based cybersecurity decision-making. *Computers & Security*, *140*, 103795. <https://doi.org/10.1016/j.cose.2024.103795>

White, J. (2022). Autonomous Reboot: Kant, the categorical imperative, and contemporary challenges for machine ethicists. *AI & SOCIETY*, *37*(2), 661-673. <https://doi.org/10.1007/s00146-020-01142-4>