Ethical Implications of a Federal Prohibition on Ransomware Payments by Hospitals

Cristian Argint

CYSE 425W: Cybersecurity Strategy and Policy

Professor Bora Aslan

Old Dominion University

October 15, 2025

Ethical Implications of a Federal Prohibition on Ransomware Payments by Hospitals

Introduction

Ransomware attacks against healthcare organizations have escalated dramatically in recent years, creating a significant tension between patient safety and national security objectives. The question of whether the federal government should prohibit hospitals from paying ransomware demands presents a complex ethical dilemma with far-reaching consequences for patients, healthcare providers, and society at large. This paper examines the ethical implications of such a prohibition through the lens of utilitarian ethics, analyzing the potential benefits and harms to multiple stakeholders.

According to the Department of Health and Human Services, ransomware incidents targeting healthcare entities increased by over 90% between 2022 and 2024 (HHS, 2024). These attacks have forced hospitals to divert ambulances, cancel surgeries, and revert to paper-based record keeping, directly threatening patient outcomes. The average ransom payment in healthcare exceeded $1.5 million in 2024, and the total cost of recovery, including downtime, remediation, and reputational damage, often reaches five to ten times the ransom amount (Emsisoft, 2024). Against this backdrop, policymakers have debated whether banning payments could deter future attacks or instead place already-vulnerable patients at even greater risk.

Utilitarian Framework

Utilitarianism, as articulated by John Stuart Mill, evaluates the morality of an action based on the extent to which it maximizes overall well-being and minimizes suffering for the greatest number of people (Mill, 1863). When applied to the ransomware payment ban, this framework requires weighing the immediate harm to patients who may be denied critical care during an active attack against the long-term societal benefit of reducing the profitability of cybercrime and thereby deterring future attacks.

The utilitarian calculus is not straightforward. In the short term, a payment ban could result in extended system outages at hospitals that experience ransomware attacks. Research by

Ponemon Institute (2023) found that healthcare ransomware attacks lasting more than five days correlated with a 20% increase in patient mortality at affected facilities. If a hospital cannot restore systems quickly and is legally prohibited from paying the ransom, the immediate harm to patients could be severe and quantifiable.

However, proponents of the ban argue that the long-term calculus favors prohibition. Every ransom payment funds criminal organizations, incentivizes additional attacks, and finances the development of more sophisticated malware (Ciancaglini et al., 2023). The FBI has consistently noted that paying ransoms encourages further criminal activity and does not guarantee the return of data. From a utilitarian perspective, if a payment ban successfully reduces the frequency of attacks over time, the aggregate reduction in harm to patients, hospitals, and the healthcare system could substantially outweigh the acute harms experienced during the transitional period.

Stakeholder Analysis

Patients represent the most vulnerable stakeholder group in this debate. During an active ransomware attack, patients may face delayed diagnoses, postponed surgeries, and limited access to their medical records. Rural hospitals and critical access facilities are particularly at risk because they typically lack the financial resources and IT infrastructure to maintain robust backup systems or absorb the costs of extended downtime (GAO, 2024). A payment ban without corresponding federal support for cybersecurity infrastructure improvements could disproportionately harm patients in underserved communities.

Healthcare organizations face a dual burden. They are simultaneously expected to maintain continuous patient care and defend against increasingly sophisticated threat actors. Many hospitals operate on thin financial margins, and the cost of implementing enterprise-grade cybersecurity measures can be prohibitive. A payment ban creates a scenario where organizations must choose between legal compliance and what their leadership may view as the medically necessary action of restoring systems as quickly as possible. This moral distress is

compounded by the reality that hospital executives bear fiduciary duties to their patients and communities.

Society as a whole has a vested interest in both a functional healthcare system and a deterrent against cybercrime. The societal costs of ransomware extend beyond immediate healthcare disruptions to include erosion of public trust in digital health infrastructure, increased insurance premiums, and the broader national security implications of funding criminal enterprises that may have ties to hostile state actors (CISA, 2024). From this broader perspective, a payment ban could serve as a necessary corrective mechanism, provided it is accompanied by investment in resilience and incident response capabilities.

Counterarguments and Limitations

Critics of the utilitarian approach to this policy raise several important objections. A deontological perspective would argue that the government has a categorical duty not to enact policies that foreseeably result in patient deaths, regardless of the aggregate long-term benefit. From this standpoint, a policy that knowingly accepts preventable patient harm in exchange for deterrence treats patients as means to an end rather than as ends in themselves (Kant, 1785). Additionally, there is no empirical guarantee that a payment ban would actually reduce the frequency or severity of attacks. Cybercriminals may shift to data exfiltration and extortion models that do not depend on payment for decryption, rendering the ban ineffective while still imposing costs on hospitals and patients (Rapid7, 2024).

Furthermore, enforcement presents practical challenges. Underground payments, cryptocurrency transactions routed through intermediaries, and the use of cyber insurance policies that may indirectly cover ransom payments all complicate enforcement. A ban that is difficult to enforce may create a two-tiered system where well-resourced institutions find workarounds while smaller, less connected hospitals bear the full burden of compliance.

Conclusion

The ethical implications of prohibiting ransomware payments by hospitals resist easy resolution. A utilitarian analysis reveals that while the long-term benefits of deterrence are compelling, the immediate and foreseeable harms to patients, particularly in underserved communities, demand careful mitigation. The most ethically defensible policy position is one that phases in a payment ban alongside substantial federal investment in healthcare cybersecurity infrastructure, incident response capabilities, and financial support for organizations during extended outages. Without these complementary measures, a standalone ban risks prioritizing abstract policy objectives over the tangible welfare of the patients the healthcare system exists to serve.

Ultimately, the ransomware payment debate illustrates a broader truth about cybersecurity policy: technical problems with human consequences require solutions that account for both the engineering of secure systems and the ethical obligations owed to the people those systems are designed to protect.

References

Ciancaglini, V., Balduzzi, M., McArdle, R., & Rosler, M. (2023). The ransomware business model and its evolving ecosystem. *Journal of Cybersecurity, 9*(1), 1-18.

Cybersecurity and Infrastructure Security Agency. (2024). *Healthcare sector ransomware: Trends and mitigation strategies*. U.S. Department of Homeland Security.

Emsisoft. (2024). *The state of ransomware in the US: Report and statistics 2024*. Emsisoft Malware Lab.

Government Accountability Office. (2024). *Critical access hospitals: Cybersecurity challenges and federal support*. GAO-24-106503.

Kant, I. (1785). *Groundwork of the metaphysics of morals*. (M. Gregor, Trans.). Cambridge University Press.

Mill, J. S. (1863). *Utilitarianism*. Parker, Son, and Bourn.

Ponemon Institute. (2023). *The impact of ransomware on patient safety and clinical outcomes*. Ponemon Institute LLC.

Rapid7. (2024). *Ransomware evolution: From encryption to multi-extortion*. Rapid7 Labs Research Report.

U.S. Department of Health and Human Services. (2024). *Report on cybersecurity incidents in the healthcare sector*. Office of Information Security.