American Journal of
Biomedical Science & Research

www.biomedgrid.com
ISSN: 2642-1747

Research Article

Risk of Medical Information Leakage through Third Parties in Japan: Trial Theory of Information Leakage Structure, Blockchain Usage, and Optimal Sanction Design Based on Game Theory

Yasuko Kawahata*

Faculty of Sociology, Rikkyo University, Tokyo, Japan

***Corresponding author:** Yasuko Kawahata, Faculty of Sociology, Rikkyo University, 3-34-1 Nishi-Ikebukuro, Toshima-ku, Tokyo, 171-8501, Japan.

To Cite This Article: *Yasuko Kawahata*. Risk of Medical Information Leakage through Third Parties in Japan: Trial Theory of Information Leakage Structure, Blockchain Usage, and Optimal Sanction Design Based on Game Theory. Am J Biomed Sci & Res. 2025 25(5) AJBSR. MS.ID.003367,* **DOI:** 10.34297/AJBSR.2025.25.003367

Received: January 27, 2025; **Published:** February 11, 2025

Abstract

This study presents a theoretical framework combining blockchain technology and game theory to address the risk structure of medical information leakage in Japan, focusing on the escalating threat of data breaches through third parties [1]. Healthcare settings face multifaceted risks of data leakage due to cyber-attacks, organizational culture, and whistleblowing challenges [2]. Additionally, Japan's delayed implementation of information education and security measures contributes to increased third-party risks [3].

This paper comprehensively examines: (1) healthcare-specific data breach factors (including fraudulent impersonation of family members and vulnerabilities in outsourcing), (2) the trade-off between blockchain's tamper resistance and anonymity [4], and (3) optimization of sanctions and monitoring costs through game theory models [5]. Furthermore, we address the necessity of multilayered countermeasures, including organizational and cultural perspectives, considering the risks of collective harassment fueled by misinformation and the involvement of children and youth [6].

In conclusion, rather than merely criticizing healthcare workers, this study emphasizes the necessity of technical and operational approaches that consider compound risks through external organizations and third parties [7]. Our objective is to provide concrete guidelines for protecting patient privacy while maintaining healthcare facility security through institutional design combining blockchain and behavioural economics approaches [8].

Introduction

This research examines the escalating structural risks of medical information leaks through third parties in Japan, analyzing current situations, structural factors, previous research, analytical approaches, and game- theoretical penalty cases [1,3]. Privacy protection in healthcare is recognized as critically important due to its handling of sensitive data directly related to life and health [9].

In Japan, incidents of medical information leakage to external parties have been increasingly reported along- side the proliferation of electronic medical records and telemedicine [10]. These leaks stem from multiple factors, including not only external cyber-attacks but also information extraction through third parties and unintended information dissemination [11].

The delay in information education during compulsory education has been identified as one factor con- tributing to medical information leakage and third- party risk issues in Japan [12]. According to the Ministry of Education's report, Japanese students rank lowest among OECD member countries in digital device us- age during classes, highlighting the need for improved information literacy

education [13]. Research from Aizu University Junior College indicates that Japan's information security education lags 10-15 years behind advanced nations like the United States [14]. Furthermore, JNSA reports note Japanese people's lack of awareness regarding information and security, describing an environment unconducive to information security industry growth [1].

Focus of the Study and Significance of Capturing Risk via Third Parties

This study focuses on the risk of information leakage not only within medical institutions, but also through the involvement of external vendors, cloud services, insurance companies, and "third parties" such as family members, relatives, and agents. This is due to the following reasons: (1) the amount of data transferred inside and outside hospitals is expanding as medical institutions increasingly utilize cloud environments and outsourcing providers, and (2) the number of external leaks, which are more difficult to detect than internal leaks, such as spoofed access by someone pretending to be a family member or relative, or fraudulent claims by someone claiming to be a legal representative or attorney, is increasing. This is one of the reasons for the in- crease in the number of external leaks, which are more difficult to detect than internal ones.

Furthermore, this study does not intend to criticize individual healthcare professionals, because there are many cases in which medical information leakage is not necessarily a problem of internal actors alone, but is caused by external attacks and incentives in the social structure. This paper will focus on how to understand the risk of such a mixture of social, technological, and organizational factors, and how to design defenses and sanctions.

Research Objectives

Our research focuses on medical information protection in Japan, particularly examining structural risks of data leakage through third parties rather than attributing blame to healthcare workers [7]. We consider sanctions design integrating blockchain technology and game theory [4,5]. The significance lies in proposing data management approaches that account for work place conditions, domestic legal frameworks, and organizational culture in medical institutions, rather than criticizing individual healthcare workers [15].

Introduction to the Study

This paper presents an initial theoretical framework combining blockchain's tamper resistance and anonymity with game theory to design optimal sanctions in medical institutions [16]. Our approach differs from existing blockchain research in the financial sector by focusing on healthcare specific organizational culture, closed environments, and risks involving socially influential individuals [17]. Medical information requires both reliability and privacy protection [18]. While blockchain technology enhances tamper resistance and data sharing capabilities, higher transaction anonymity may increase the risk of overlooking information leaks by internal stakeholders [19]. As a countermeasure, we propose optimizing sanction design through game theory applications within practical operational constraints of medical institutions [20].

Therefore, this paper offers novelty in three integrated perspectives: (1) analyzing healthcare-specific risk structures (whistleblowing difficulties, family dynamics, organizational hierarchies) [2], (2) considering both tamper resistance and anonymity aspects of blockchain [21], and (3) attempting optimal sanction design using game theory models [5]. Particularly, game theory analysis for the healthcare sector remains underdeveloped, and our research aims to provide concrete guidelines for setting sanction levels and monitoring costs.

Challenges and Risks in Medical Information Protection

The healthcare sector handles highly sensitive personal information, including patient data and confidential healthcare worker information that directly impacts life and health [7]. While recent information society has rapidly advanced electronic medical records and telemedicine systems, various risks have emerged, including cyber-attacks and unauthorized data removal by internal stakeholders [11]. Information leaks can severely impact not only the individual but also their family and related parties [22].

Recent Survey Results on Information Leakage Incidents

According to JNSA reports, there were 443 personal information leakage incidents in 2018, with 28 cases (6.3%) occurring in the medical/welfare sector [1]. Primary causes included loss/misplacement, operational errors, and unauthorized access. IPA's survey revealed that in 2014, external attacks accounted for 49% of global data breaches, while internal misconduct comprised 8% [3].

Challenges with Cases Involving Socially Influential Individuals

In cases involving socially influential individuals, public sanctions may exacerbate damage, necessitating closed sanctions and long-term monitoring systems [23]. When influential individuals are hospitalized, leaked medical data can trigger media attention, potentially disrupting hospital operations and affecting other patients [10]. Additionally, when management is involved in breaches, organizational hierarchies can impede whistleblowing effectiveness [2].

Ethical Blind Spots in Violations

Many violators leak information without fully recognizing their actions as violations [24]. This awareness gap cannot be adequately addressed by traditional prisoner's dilemma models, requiring frameworks incorporating behavioral economics and incomplete recognition models [7]. For instance, healthcare workers might casually share patient information with family members without consent, potentially leading to secondary damages through resale or social media dissemination [6].

Information Protection Challenges in Other Sectors

The financial sector faces risks of fraud and credit score manipulation through personal information misuse [25]. Social media platforms struggle with privacy violations and misuse of user data, as exemplified by the Cambridge Analytica incident [6].

Cambridge Analytica Case Study (2018)

The Cambridge Analytica incident demonstrated significant implications for personal data misuse [6]. The company collected Facebook user data without proper consent for political campaign purposes [26].

Data Collection Methodology and Impact

The data collection utilized Facebook's API to gather profile information, friend lists, and posts [11]. The impact affected approximately 87 million users by 2018, as shown in Table 1.

Table 1: Progression of Facebook Data Collection Impact (Estimation).

Year	Affected Users (Millions)
2015	10
2016	30
2017	50
2018	87

Legal Consequences

The incident resulted in significant regulatory changes and fines for both Cambridge Analytica and Facebook [26]. Facebook implemented enhanced privacy protection measures and faced stricter data management regulations [6].

Implications for Healthcare Data Protection

The Cambridge Analytica case provides valuable lessons for healthcare data protection [7]. It emphasizes the need for: Robust consent mechanisms [18]. Third-party access controls [4], Enhanced privacy protection frameworks [11].

Medical Information Protection Systems and Penal- ties Across Countries

The following sections analyze medical information protection systems in various nations [18].

Comparative Overview

Table 2 presents a comparison of medical information protection systems and associated penalties across major nations.

Table 2: Comparison of Medical Information Protection Systems and Penalties by Country.

Country	Primary Laws/ Systems	Key Penalties and Notes
USA	HIPAA†	Tiered system: $100- $50,000 per incident, annual cap $1.5M; criminal penalties for severe violations [18]
UK	NHS management system, GDPR compliance	Max: €20M or 4% of global revenue integrated data protection framework (GDPR/Data protection act) [26]
Japan	Personal Information Protection Act	Imprisonment up to 1 year or fines up to ￥500,000; corporate fines up to ￥100M [1]
India	Developing data protection laws	Case-by-case handling due to immature legal framework [6]

Blockchain and Security

Blockchain technology enhances tamper resistance and reliability through distributed ledger technology [16]. In blockchain networks, multiple peers (nodes) collectively validate transactions and append approved data chronologically, making unauthorized modifications extremely difficult [27].

Recent developments incorporate advanced cryptographic techniques like multi-signatures, Zero Knowledge Proofs (ZKP), and homomorphic encryption into blockchain systems [21,28]. For instance, multi-signature functionality prevents critical operations without multiple authorized signatures, deterring internal fraud. ZKP enables verification of transaction validity without revealing specific content, while homomorphic encryption allows computation on encrypted data without decryption.

Application to healthcare information management offers enhanced tamper resistance and audit capabilities while protecting patient privacy [17]. However, high anonymity levels may benefit malicious actors [19]. While advanced cryptography can balance privacy and transparency, ZKP and homomorphic encryption often require substantial computational resources, potentially challenging scalability in large healthcare institutions.

Notes on Operational Costs and Burden

When introducing blockchain technology into the medical field, initial and operational costs for system construction and maintenance, as well as training and manual maintenance costs for hospital staff, may be higher than expected. In particular, the following points should be noted.

Node operation and network maintenance: To function as a distributed ledger, multiple nodes must operate stably, and server management costs on the cloud or on-premise will be high.

Computational Resources and Time Delay: When performing high-load operations such as zero-knowledge proofs and homomorphic ciphers, there is concern that the response time will slow down and interfere with workflow of the clinical site.

Assurance: Considering the medical professionals operate the system during their busy schedule, it is essential that the operation screen is easy to understand and that there is a support system in case of trouble.

Updates and Security Patches: Every time the blockchain or related libraries are updated, the hospital system also needs maintenance and revalidation, which could incur additional costs.

When evaluating all of these factors together and optimizing sanction design and audit costs in a game- theoretic manner, it is important to consider in advance what level of operational burden is actually acceptable.

Overview of Blockchain Security and Healthcare- Specific Challenges

Tables 3 and 4 summarize key aspects and challenges. Key considerations for medical information blockchain implementation include: - Optimal anonymity levels balancing privacy and traceability - Access control and monitoring system enhancement within cost constraints -Sanction level determination considering deterrence and organizational impact [4]. These elements require game-theoretical analysis for optimal implementation in healthcare settings [5].

Table 3: Key Aspects of Blockchain and Security.

Element	Description
Basic Structure	Distributed ledger technology enhancing tamper resistance and reliability through peer validation [16,27]
Tamper Resistance	Modification requires recalculation of all subsequent blocks, creating computational barriers and inconsistencies with legitimate nodes
Advanced Cryptography	Integration of multi-signatures, zero- knowledge proofs (ZKP), and homomorphic encryption for enhanced privacy preservation [21,28]
Multi signature	Requires multiple authorized signatures for transaction validation, preventing centralized control and internal fraud
Zero knowledge Proofs	Enables transaction validation while maintaining data privacy, verifying compliance without revealing specifics
Homomorphic Encryption	Permits computational operations on encrypted data, maintaining confidentiality throughout processing
Healthcare Applications	Management of electronic health records with immutable access logs and enhanced audit transparency [17]
Anonymity Risks	High anonymity levels may complicate tracking of internal data breaches [19]

Table 4: Healthcare-Specific Challenges in Blockchain Implementation.

Challenge	Description
Anonymity Balance	Balancing patient privacy protection with traceability of unauthorized access
Access Control	Defining legitimate access rights while optimizing surveillance costs and detection rates
Sanction Design	Optimizing penalties to deter violations without negatively impacting organizational culture
Interorganizational Access	Implementing unified access controls across different healthcare institutions while preventing data breaches
Audit Transparency	Establishing clear audit trails and accountability despite immutable blockchain records
Staff Training	Ensuring proper understanding of operational rules and prevention of authorization misuse
Patient Consent	Developing informed consent mechanisms for blockchain-based data sharing

The implementation of blockchain in healthcare requires balancing three key considerations [16,19]:

a) **Anonymity Level Optimization** - High anonymity enhances patient privacy but impedes tracking - Lower anonymity compromises confidentiality

b) **Access Control and Monitoring** - Enhanced surveillance increases detection rates - Cost-benefit analysis of monitoring systems - Cross-organizational access protocols

c) **Sanction Design** - Penalty optimization for deterrence - Impact on organizational culture - Compliance motivation factors.

Blockchain technology offers robust tamper resistance and enhanced security through distributed validation [27], but implementation must consider healthcare specific requirements (Table 3).

-Patient data confidentiality - Cross-institutional collaboration - Regulatory compliance - Operational efficiency.

The optimal framework requires balancing technical capabilities with practical constraints, incorporating game theory principles for effective sanction design [5,20].

While blockchain technology offers significant potential for securing medical information [16], practical implementation requires careful consideration of healthcare operational dynamics:

Key Implementation Considerations: - Balancing privacy protection with operational transparency - Optimizing detection mechanisms within resource constraints - Designing effective sanctions that maintain organizational morale.

Technical Architecture Requirements: - Multi- signature protocols for distributed authorization - Zero- knowledge proofs for privacy-preserving verification - Homomorphic encryption for secure data processing [28].

Healthcare-Specific Protocols: - Patient consent management systems - Cross-institutional data sharing frameworks - Audit trail mechanisms with clear accountability.

The success of blockchain implementation in healthcare depends on integrating these elements while addressing: 1. Scalability for large medical institutions 2. User interface simplification for medical staff 3. Compliance with regulatory frameworks [17].

These factors necessitate ongoing research into optimal system design that balances security with usability in healthcare environments [19].

Countermeasures against Maximizing Illicit Gains from Medical Information Leakage

In recent years, cases have been reported of individuals impersonating someone else to misuse health insurance cards. For example, there have been confirmed incidents in which a stolen health insurance card was used to assume another person's identity in order to obtain a copy of their resident registration certificate, which was subsequently used to open a bank account for fraudulent transactions. Moreover, in a session of the House of Representatives Cabinet Committee in 2019, abuses involving impersonation using insurance cards were highlighted, underscoring the importance of utilizing identification with a photograph for verification [13]. These examples show that fraudulent activities using counterfeit or stolen insurance cards continue to exist, and there are concerns that such schemes will increase in the future. Consequently, strengthening personal identification at medical reception desks has become a pressing issue (Table 4).

Patterns of Leakage Where Malefactors Have Substantial Advantage and Accusation is Difficult

When contemplating the leakage and exploitation of medical information, there exist attackers and brokers determined to maximize their profits, while the entities responsible for prevention (e.g., healthcare providers, service providers) do not always possess sufficient information or resources. From a game-theoretic perspective [20], the following structure comes to light:

a) **Attacker (Abuser) Payoff:** Financial or political benefit derived from theft or resale of information.

b) **Defensive Costs (Healthcare Providers, ISPs, etc.):** Rising expenses for system fortification, staff training, awareness campaigns, and audits.

c) **Difficulty in Imposing Penalties after Information Leakage:** Due to the obscured nature of the leakage and external pressure not to disclose incidents, sufficient deterrence is often not achieved.

In such circumstances, there is a high risk of drifting toward an inequitable equilibrium in which an attacker' s payoff function grows while the defensive side alone faces escalating costs. Furthermore, if a medical institution discloses its own victim status, it risks a decline in credibility, thereby creating an incentive to conceal the breach. Consequently, the attacker's comparison between the "risk of punishment" and the "gain from misuse" may remain in favor of the latter, leading to a potentially entrenched structure where malicious activities continue to be profitable.

It has been noted that the leakage of medical information often occurs in environments where offenders seeking profit enjoy a genuine advantage, and public condemnation is not easily carried out. Despite the increasing number of preventive measures in medical facilities—such as the installation of security cameras and the strict management of visitor logs—there has been no shortage of severe instances of information theft. In what follows, we summarize and discuss patterns in which it is particularly difficult for relevant parties to report wrongdoing or to hold offenders accountable.

Impersonating Family Members or Relatives

A relatively foreseeable type of fraud in the healthcare setting involves obtaining patient information by pretending to be a family member. For instance, an individual without any actual blood or familial ties might gain clearance at the reception or enter a waiting

room or patient room by masquerading as a close relative. Although hospitals take stringent measures when admitting or discharging patients, incidents of unauthorized access have been reported. Alternatively, there may be cases in which a genuine relative, without the patient 's consent, intentionally obtains sensitive in- formation and sells it. In these situations, healthcare personnel may assume that "because they are family, sharing information poses no issue," creating a system where illicit acquisition is less likely to surface.

Legitimate Relative but with Specific Intent

Even if an individual holds a formal position as a family member or close kin, he or she may harbor the intent to exploit medical information for financial gain (e.g., insurance fraud or monetary benefits). Such an individual might utilize the patient 's healthcare data to negotiate with insurance companies or to file false claims for various benefits. Staff and physicians, thinking "they are immediate family," may be less inclined to question the details being requested, enabling an atmosphere conducive to abuse. Moreover, even if the patient notices and wishes to raise an alarm, familial ties or the desire to avoid internal disputes can deter them from taking corrective action.

Collusion or Bribery of Internal Staff

External perpetrators may bribe hospital employees, who then deliberately remove confidential data. Regardless of how rigorously security cameras and visitor log management are implemented, if staff have legitimate system access, there remains a risk that they may improperly copy data under authorized credentials. Additionally, such insider misconduct is difficult for outsiders to detect. Reporting it can be hindered by fears of retaliation among coworkers, reducing the likelihood of whistleblowing within the organization.

Access Requests by Individuals Posing as Legal Representatives or Attorneys

Medical institutions may receive requests for disclosure of patient information from proxies or attorneys acting on the patient's behalf. If the institution's verification of documents and identity is insufficient, an attacker could obtain crucial data under the guise of legal procedures. Notably, if a staff member who is not fully versed in the Medical Care Act or the Act on the Protection of Personal Information processes the request, the fraudster can exploit the ambiguity surrounding the authenticity of the submitted forms or the validity of a seal, resulting in uncertain confirmation of patient consent.

Forged Patient Status and Misuse of Health Insurance for Resale

In some instances, individuals may present a falsified or stolen insurance card or ID card at a healthcare facility and then procure test results and prescription details for resale. These individuals exploit ever improving falsification methods alongside the chaotic nature of crowded reception desks, choosing moments when staff may lack sufficient time for rigorous verification. When tied to fraudulent insurance claims, the perpetrators can make even greater profits, and there is no zero possibility that organized criminal syndicates systematically dispatch such patients.

Leakage at Cloud Services or External Contractors

When a healthcare provider stores electronic medical records and imaging data on external cloud platforms, personnel at these third-party services may commit unauthorized access and remove data. Alternatively, if the cloud's security measures are weak, hacking or ransomware attacks can lead to massive data breaches. Even then, due to contractual limitations with the service provider, a hospital may offer only limited disclosure of the incident and fail to sufficiently alert the patients involved. Here, the institution tends to prioritize actions that prevent further escalation, and fear of legal liability or reputation damage can foster a strong incentive to keep incidents under wraps.

Partial Acquisition of Past Diagnostic or Lifestyle Data

Even without gaining access to complete medical records, acquiring fragments of a patient's past hospital admissions or periodic test results can allow offenders to intimidate the individual by threatening to reveal their personal health history. Such disclosure of personal habits or mental health details can compromise the patient's social standing or be leveraged for extortion. Because only partial data is taken, healthcare providers may downplay the incident, believing "the entirety of the data was not breached," which can make it less likely for perpetrators to face timely accusations.

Environments Where Internal Whistleblowing or External Reports Are Unfeasible

In Japan and other parts of East Asia, strong hierarchical structures and the risk of retribution toward informants have been cited as reasons why internal reporting systems frequently fail [2]. Even if a nurse or a technician discovers wrongdoing, higher management may opt to conceal it to "avoid causing anxiety for patients," or they may inflict negative personnel actions on the whistleblower, effectively discouraging reports. As a result, an environment develops in which offenders continue to have the upper hand for an extended period.

For Peace of Mind and Safety The risk of medical information leakage arises not merely from "external hacking" but also from a wide range of scenarios including impersonation by relatives or associates, collusion with internal staff, misrepresentation by external contractors, and fake patients. Offenders gain substantial advantage in such complex environments because interpersonal trust and familial bonds, coupled with insular workplace cultures, can make whistle blowing and public disclosure extremely difficult. Al- though reinforcing information security systems and strict verification at reception are crucial, such efforts alone are insufficient to fundamentally prevent malicious data leaks without additional measures to protect whistleblowers and foster a culture of accountability. In order to ensure that patients, healthcare professionals, and society at large can utilize medical services with confidence, it is essential to approach the issue with both technological safeguards and thorough oversight—both internally and externally.

Documented Cases of Medical Information Leakage and Research Reports

Specific Risks of Data Leakage

Healthcare environments have increasingly embraced IT solutions such as electronic medical records, diagnostic imaging systems, and telemedicine, which necessitate data exchange through the internet. However, the number of information leakage incidents triggered by cyberattacks and insider misconduct remains significant. The following risks have been noted in the literature [11,14,9,29]:

a) **System Outages and Personal Data Leaks Caused by Ransomware:** Healthcare facilities may be crippled, requiring substantial cost and time for recovery.

b) **Unauthorized Viewing by Insiders:** Patient's records are inappropriately accessed due to flawed authority management or moral hazards.

c) **Breaches Originating from Third-Party Contractors:** Security policies at cloud service providers or data centres may be inadequate.

Such lapses can have devastating impacts on medical staff, patients, and their families, and the structural challenge of keeping these leaks hidden for long periods has been highlighted [29]. Furthermore, once data is leaked, resale or dissemination makes prosecutions difficult from a game-theoretic standpoint [20].

Overview of Prior Research

Provides a comparative summary of prominent research on safeguarding medical information.

Technical Approaches Under Consideration

Encryption and intrusion detection systems remain critical measures against cyberattacks and unauthorized access [11]. Recently, researchers have explored multi-faceted methods such as AI-driven anomaly detection and blockchain-based tamper-proofing [19]. In addition, network architectures like VPNs and zero-trust frameworks, which redefine internal-external boundaries, have garnered attention, with a growing number of reported implementations in hospitals [29,14] (Table 5).

Table 5: Major Research Studies on Medical Information Leakage.

Study	Key Focus	Principal Findings
Anderson (2006) [14]	Investigation of security protocols within healthcare institutions	Quantitatively demonstrated that authority management and human error are significant contributing factors
Sicari et al. (2015) [11]	Security and privacy in the IoT era	Emphasized the need for multi-layered defences against cyberattacks and data theft in healthcare equipment
Nat Zone (2024) [9]	Comparative study of HIPAA regulations and their influence on Japan	Analyzed how stringent U.S. penalties and guidelines are shaping Japanese security standards
IT and PC Terminology Guide (2024) [29]	Compilation of HIPAA regulations	Provided concrete data security requirements and compliance recommendations for healthcare professionals
Tirole (1988) [20]	General research on game theory	Suggested applications to incentive structures and fraudulent activities in medical settings

Operational and Societal Challenges

Governance and Training

Regardless of the sophistication of technical measures, if healthcare workers are not properly trained or do not comply with operational guidelines, the risk of information leakage remains high [9]. Several operational efforts have received increased focus

i. Regular security and compliance training

ii. Strict management of access privileges and review of audit logs

iii. Establishment of protocols for incident reporting and public disclosure

International Frameworks and Comparisons

Numerous precedents, including Europe's GDPR and the U.S. HIPAA, legislate the protection of personal data, including medical information [26]. Conversely, in countries such as India, whose legal institutions are still developing, there is a perceived lack of cohesive regulation, highlighting the importance of international collaboration and support [9].

Efforts to Safeguard Rights and Reassurance in the Healthcare Setting

As discussed above, numerous types of threats can lead to medical information breaches—ranging from impersonating relatives to internal collusion. These risks are not solely due to vulnerabilities such as external hacks or deficient security measures, but also arise from intricate factors such as family dynamics, reluctance to report unethical activities, and a secretive organizational climate. Nevertheless, healthcare settings should guarantee that families, medical staff, and patients can engage in medical care in a secure and sup-

portive environment. This section explores preliminary proposals to address these issues without becoming excessively cautious, while still implementing effective safeguards.

Balancing Accurate Risk Awareness with Composed Responses

It is essential that healthcare personnel recognize the seriousness of data leaks but avoid becoming overly

suspicious. For instance, the reception and visitation processes should be streamlined to confirm a visitor's identity, yet interactions with patients and families should remain smooth. One effective approach is to spell out procedures for "how to respond if suspicious behavior is observed" in the official operation manual. This allows for calm and systematic responses to suspected fraud without needlessly undermining patient and family trust.

Whistleblower Protection and Incentives for Reporting

Staff members who detect wrongdoing in a healthcare facility may hesitate to report it for fear of retaliation or personnel disadvantages. Thus, instituting frameworks that protect whistleblowers and providing clear instructions on how to report suspected incidents are crucial. From a behavioral economics perspective [8], establishing mechanisms (e.g., anonymous hotlines or third-party whistleblowing channels) can lower the psychological barriers to reporting. This study proposes that such strategies can strongly encourage staff to come forward.

Collaboration with Local Partners and External Audits

Medical facilities should not operate as closed systems but rather partner with local health offices, other hospitals, legal associations, and government auditing bodies to create an environment conducive to third- party reviews. By sharing best practices in medical information management through collaborative research and conference presentations—and by introducing up- to-date security technologies and internal control models—healthcare facilities can better address risks that are beyond the capacity of a single institution. Such cooperative efforts help dismantle excessive secrecy and foster both robust data protection and the safeguarding of patient rights.

Multilevel Education and Cultural Development

Hospitals consist of diverse roles, from nurses and administrative personnel to physicians and senior management, each of whom perceives data leakage risk differently. Hence, targeted training for each role is required. Beyond teaching staff about security technologies and policies, case studies or simulations can help them understand "why data protection is crucial to patient safety and organizational credibility." This approach is expected to foster a culture of addressing risks rationally, without succumbing to undue anxiety.

Discussion

Healthcare facilities must be places where patients, their families, and medical professionals can focus on treatment and care with assurance. While measures to counter information leakage may become excessively cautious and potentially strain patient provider relationships, various initiatives—including whistleblower support, multilevel education, and collaboration with external auditors—can diminish the advantage enjoyed by malicious actors. At the same time, these steps strengthen privacy and reassurance for all stakeholders. Employing a combination of technological, organizational, and societal methods is vital for striking a balance between effective data protection and a safe, hygienic clinical environment. Ongoing research, surveys, and practical trials in these domains will be indispensable in achieving these objectives.

Research Cases on the Issue of Medical Information Leakage and the Difficulty of Reporting in Insular Environments

In the previous research notes, discussions focused on the exceptionally sensitive characteristics of medical data and the serious repercussions if such information is compromised. Debates on this matter can be traced back to around the 1980s, when the use of internet technologies expanded across corporate and academic institutions. In healthcare settings, where patient and family privacy is deeply implicated, minimizing the risk of data breaches has become critically important from a societal perspective. Nevertheless, a highly closed organizational culture in hospitals, a lack of adequate reporting mechanisms, and insufficient whistleblowing infrastructure can converge to make it extremely difficult to report and deter malicious behavior. Moreover, it is evident that not all healthcare facilities enjoy the same level of technological or informational resources. In what follows, this paper addresses both the problem of medical information leakage and the challenge of reporting wrongdoing within these isolated environments.

Risks and Consequences of Medical Information Leakage

Handling Highly Sensitive Data

Because medical data contains inherently private information—such as an individual's medical history, diagnoses, prescription records, and genetic details— its disclosure may result in damages that are extremely difficult to reverse [14]. Additionally, the spread of electronic medical records and telemedicine technologies has led to an expanded volume of data transmitted over networks, thus exacerbating risks related to external hacking and ransomware attacks that can incapacitate systems [11].

Impact on Both Patients and Medical Staff

A breach of medical records can pose not only an invasion of privacy for patients, but also trigger social discrimination and economic harm. Furthermore, healthcare professionals also face significant repercussions: the risk of retaliation against internal whistleblowers, as well as potential censure for lapses in oversight, can incentivize individuals to cover up wrongdoing rather than report it [9]. Such a pressurized setting can impede both the discovery of breaches and the act of raising alerts.

Information Misuse and Difficulty of Disclosure in Closed Environments

Structural Challenges Specific to the Healthcare Setting

Healthcare workplaces bring together high-level specialists whose decisions can be a matter of life or death, often fostering a strong hierarchical structure within the organization. In many instances, if internal whistle- blowing or suspicion arises, it may be contained internally out of concern for "creating patient anxiety" or "disturbing organizational harmony" [7]. In East Asian regions—including Japan—a cultural emphasis on maintaining organizational order can further amplify the closed nature of the environment, making it problematic to report externally, even where serious wrongdoing or data misuse is suspected.

Underdeveloped Reporting Infrastructure and Associated Risks

One reason for the difficulty in reporting is that existing frameworks—such as legally mandated whistle- blowing programs or hotlines—often fail to operate effectively in practice [24]. Additionally, when the ICT infrastructure or security auditing systems within a healthcare institution are inadequate, ongoing data exploitation may remain undetected, allowing potential damage to persist. Even under the U.S. HIPAA regime, where healthcare workers might attempt internal whistleblowing upon suspecting improper behavior, there is persistent concern that organizational leaders, who already know the reporting channels, could subject the informant to retaliation [29].

Other Concerns and Research Cases

Non-public Penalties and Closed-Door Sanctions for Information Leakage

As noted in previous discussions, when the individual involved is a high-profile figure or the offense is exceptionally egregious, making the penalty public might have the undesirable effect of backfiring; thus, some argue that prolonged or discreet punitive measures, as well as covert monitoring, may be necessary [20,5].

However, when such closed-door disciplinary measures are actually implemented, they often occur solely within the organization, making it difficult for third- party oversight to function effectively. In healthcare settings, where punishments and personnel actions are rarely disclosed, neither patients nor external institutions can gain a clear picture of the internal situation, thus creating a dilemma wherein misuse might continue unchecked.

Research Example: Psychological Barriers to Whistleblowing in Japanese Healthcare

A qualitative investigation by *Takemura* [2] examined psychological obstacles to whistleblowing among nurses and hospital staff in Japan. According to the interview data, even if individuals suspected wrong- doing, many would refrain from reporting because they "consider their colleague's or superiors positions" or fear that "the hospital 's reputation might suffer, discouraging patients from seeking care." Consequently, actual breaches or unethical acts may persist under tacit acquiescence from some members of the organization.

Research Example: Growth of Electronic Medical Records and Increasing Avenues for Leaks

Sicari et al. [11] highlight that as the deployment of IoT technologies accelerates in medical de- vices and sensor networks, vulnerabilities not covered by conventional security models are expanding. In particular, the greater the adoption of electronic patient records and remote medical devices, the more intricate the communication pathways become, making breach monitoring more challenging. In such scenarios, determining who should be notified and where responsibility lies becomes murky, ultimately rendering the reporting of data misuse even more difficult.

The challenge of preventing and identifying medical information breaches involves a complex interplay of technological risks and social/organizational elements. Healthcare institutions in particular, characterized by tight cooperation among highly trained specialists and hierarchical structures, tend to deter both internal and external disclosures of misconduct. Moreover, when closed-door sanctions are conducted in an isolated setting, outside transparency and third-party inspections can be obstructed. Addressing these problems therefore calls not only for reinforced technological defenses and deterrent measures but also for robust internal controls that protect whistleblowers, cultural reforms within organizations, and mechanisms for broader societal information sharing. Drawing from these research findings, it is crucial to approach medical data security by aligning international frameworks and leveraging insights from behavioral economics to prevent leakage and to contain damage once it occurs.

Information Health Perspective

Information Health, an emerging concept, has recently been proposed for the "sound" administration of electronic health records and large-scale medical data [10]. Specifically, the objectives include: (1) ensuring data authenticity, (2) safeguarding privacy, (3) managing information ethically, and (4) ultimately improving patient outcomes over the long term. A number of hospitals in Europe and the United States have begun pilot initiatives that incorporate Information Health into their audit processes.

As discussed in the earlier research notes, the prevalence of closed hospital cultures can hinder whistle- blowing. In addition, healthcare organizations face technical threats—such as hacking and ransomware— and institutional shortcomings—like underdeveloped reporting channels and weakened governance—that collectively make it difficult for data breaches to surface. Here, we examine how securely managing patient records to avoid improper disclosure aligns with improving Information Health. This concept, referring to the maintenance and circulation of electronic or digitized medical information in a safe condition, includes requirements for reliability and data confidentiality [10].

Protecting Medical Data and Strengthening Information Health

Several perspectives show why safeguarding medical data supports Information Health

A Sound Information Environment that Upholds Patient Autonomy

Patients must have access to trustworthy information systems in order to correctly comprehend their medical condition and available treatment options [14]. Yet, if there is a high probability that an individual's medical history or genetic data could be leaked externally, patients may hesitate to disclose information, jeopardizing the process of informed consent. To achieve Information Health, data breaches or other abuses must be minimized so that patients can make autonomous decisions without unease.

Cultivating Professional Trust and Ethical Practice Among Healthcare Workers

When healthcare professionals rigorously follow data protection protocols, trust between patients and families is reinforced, and adherence to ethical standards increases throughout the organization [2]. In insular environments, internal whistleblowing and reporting of misconduct are often viewed as taboo. Consequently, instituting robust internal controls that also safeguard whistleblowers can directly advance the goals of Information Health. An effective whistleblowing framework can detect leak risks and unethical conduct early, thereby raising the organization's literacy and ethical awareness [24].

Enhancing Organizational Culture and Collaboration with Society

As noted by *Sicari, et al.* [11], while the widespread adoption of electronic records and IoT devices dramatically expands data sharing capabilities among diverse stakeholders, it simultaneously multiplies possible points of leakage. From the standpoint of Information Health, international cooperation and standardization are necessary to securely and efficiently manage such complex networks of information flow. A culture of "non-concealment" and "accessible reporting" also fosters transparency, paving the way for collaboration with external auditors and third-party scrutiny, ultimately enhancing the credibility of health care providers.

Practical Research Examples

Securing Medical Information Systems and Improving Health Outcomes

Maxwell, et al. [10] investigated electronic medical record deployments across multiple health care institutions. Their findings indicated a correlation between reduced leak risks and improvements in patient outcomes. When highly sensitive diagnostic data is shared securely, inter-hospital collaboration is streamlined, hastening treatment decisions. However, facilities with inadequate funding for security or undeveloped whistleblowing processes experienced limited benefits from system implementation. These results underscore that reinforcing data governance—aligned with the concept of Information Health—can positively impact patient welfare.

International Frameworks and the Use of Big Data in Healthcare

International frameworks such as the European GDPR and the U.S. HIPAA substantially influence the handling of medical data. *Morley, et al.* [6] studied various cases of using large-scale healthcare data under GDPR, concluding that strict data-protection measures can coexist with research objectives, aligning closely with the principle of Information Health. The presence of rigorous penalties compels hospitals and research institutions to take privacy and security seriously, enabling data sharing under safer and more trustworthy conditions.

Organizational Reform via Behavioral Economics

Among the many factors fueling risks of medical data breaches, difficulty in reporting misconduct and insular cultural attitudes loom large. *Bazerman and Tenbrunsel* [24] emphasize, from a behavioral economics and behavioral ethics viewpoint, that it is not enough to build whistleblowing frameworks alone; organizations must foster an environment that encourages expressing concerns and lowers psychological barriers to speaking up. Incorporating such strategies in healthcare settings can bolster internal controls essential for Information Health. Concrete examples include regular workshops among nursing staff and the empowerment of ethics committees, measures reported to have achieved positive outcomes [2].

By applying both technical and organizational safeguards to mitigate medical data breaches, healthcare institutions not only strengthen the sense of security for patients and providers, but also contribute to advancing Information Health. This concept is broad based, integrating not only data protection and privacy but also social and ethical foundations. Future research and practice should thus explore solutions that address insufficient reporting mechanisms and organizational governance in closed settings, drawing on both technological safeguards and incentive models from behavioral economics. Aligning with international data protection guidelines and sharing cutting edge methods could further elevate medical data security.

Challenge: Approaches to Address the Risks of Data Breaches and Reporting

Until now, discussions of medical data breaches have commonly invoked game-theoretic models, which assume that a perpetrator seeking to leak information aims to maximize personal gain and that punishment design becomes problematic when enforcement is difficult. However, analyzing real-world problems can profit from methods extending beyond game theory and integrating various academic disciplines. This section proposes non-game-theoretic approaches to situations in which bad actors can readily pursue private benefit, while external condemnation proves challenging. Related research examples are introduced accordingly.

Behavioral Economics and Behavioral Ethics Approaches

Nudge Theory (Behavioral Economics)

Originating from *Thaler and Sunstein* [8], Nudge Theory assumes that individuals are not entirely rational and are influenced by cognitive biases. The approach aims to incorporate subtle "nudges" into policy and system design to direct personal choices toward more desirable outcomes. For instance, in the context of managing medical information, an interface could be designed to automatically display warning messages at a stage where users are likely to proceed with high-risk behaviors. In so doing, it promotes a moment of reconsideration that might deter data leaks.

Behavioral Ethics and Analysis of Blind Spots

According to *Bazerman and Tenbrunsel* [24], ethical lapses within an organization can be overlooked due to "blind spots" formed by individual cognitive biases. In closed communities of high specialization— such as healthcare institutions—external critique or internal whistleblowing is less likely to surface. Consequently, beyond models strictly based on rational payoffs (e.g., game theory), incorporating insights from behavioral ethics can spotlight organizational culture and psychological barriers, thus facilitating the development of more comprehensive deterrents and incentives for reporting wrongdoing.

Sociological and Organizational Approaches Organizational Culture and Whistleblower Protection Mechanisms

Weick and Sutcliffe [15] highlight the importance of "resilient operations" in high-risk environments, including healthcare institutions. Organizational resilience refers to embedding in the corporate culture the capacity for rapid detection and intervention once a problem arises. Where data leakage threats are substantial, the implementation of whistleblower or hotline systems that allow staff to report safely (e.g., third-party hotlines, anonymous reporting) can bolster transparency and expedite countermeasures.

Social Network Analysis of Power Structures

The Social Network Analysis (SNA) method proposed by *Borgatti,* et al. [23] examines how power and information flow within an organization. Because healthcare settings typically involve intricate hierarchies and complex vested interests, visualizing the power relations that might facilitate or obstruct reporting can clarify who holds sway over data leaks and who might deter whistleblowers. This technique also enables an external, macro-level view of power imbalances that might elevate the risks of retaliation.

Applying Cryptography and Blockchain

Kshetri [19] underscores the strong tamper- resistance and traceability features of blockchain, suggesting its applicability to medical data administration. By ensuring that, once data is compromised, the access route and usage records remain permanently logged, it becomes more feasible to track and intercept misconduct before a perpetrator can maximize illicit gains. Although this measure can be interpreted in game-theoretic terms as "boosting the probability of detection," in practice it is an engineering strategy centered on decentralized ledger technology, diverging from purely game-theoretic methodologies.

Machine Learning and Anomaly Detection

Within the broader call for multi-layered defenses— especially in IoT and medical device networks—*Sicari, et al.* [11] propose real-time anomaly detection systems (IDS) that leverage machine learning to monitor network traffic, user logs, and device behavior. Such systems can analyze user actions and trigger alerts before an attacker fully capitalizes on a leakage. Nonetheless, this approach hinges on organizational and financial support for system design and maintenance.

Criminology and Deterrence Theory

General and Specific Deterrence in Criminology

Classical criminological theories traceable to Beccaria and Bentham emphasize general deterrence by intensifying punishment—a notion bearing some resemblance to game-theoretic strategies. However, criminology also accentuates the importance of specific deterrence in handling repeat offenders and organized crime groups [20], for instance by introducing rehabilitation programs and protective oversight structures in addition to punitive measures. Insights from this field can inform how organizations might execute effective deterrent mechanisms when condemnation carries substantial risk.

Case Studies

Successful Examples of Organizational Culture Reform

Ostrom [30] examined the tragedy of the commons, an issue that can extend to the management of healthcare data conceptualized as a "shared resource." Her work suggests that, by instituting collective rule making and fostering a culture of mutual oversight, organizations can suppress misconduct without relying solely on external enforcement. This success hinges upon cultivating trust within the organization and fostering an environment where reporting violations is feasible—an area where social or cultural consensus- building can supplement game-theoretic approaches.

Precedent for Blockchain Implementation

Kshetri [19] describes a case in which blockchain was adopted as a platform for the healthcare and insurance industries, permanently recording data access logs in a tamper-proof form. Even if insiders attempt to manipulate data, the unchangeable audit trail facilitates rapid detection, eroding the prospective benefits of a data breach before the offender can fully exploit the information. From a practical standpoint, the system introduces an engineering and policy based barrier that operates alongside—rather than strictly within—game-theoretic frameworks.

In environments where offenders seeking personal gain hold a genuine advantage and condemnation is challenging—such as in medical information breaches—exclusive reliance on game theory might not produce sufficient deterrence. Hence, complementary approaches are required: behavioral economics and behavioral ethics to address cognitive biases and blind spots; sociological and organizational strategies to bolster internal whistleblower protection; and technical solutions such as blockchain or machine-learning based anomaly detection. Ultimately, it is crucial to synthesize these multiple approaches in consideration of real-world conditions, user behaviors, and the broader sociopolitical context. As the literature indicates, an all-encompassing strategy—incorporating interpersonal relationships within the organization and external technological support—represents the key to preventing leaks and encouraging whistleblowing.

For instance, even if new security systems or blockchain solutions are deployed, busy physicians and nurses may not use them effectively in a demanding clinical environment. During the initial deployment stage, additional workloads might overwhelm staff, and employees with low compliance awareness may feel that these measures simply add "unnecessary tasks." Consequently, not only is a top-down push important, but also iterative refinements based on user feedback can enhance usability and encourage more constructive attitudes toward data protection.

Anonymity Risks in Blockchain Implementation and a Game-Theoretic Perspective

As shown by *Kshetri* [19], there are instances in which blockchain technology is deployed as a joint platform for healthcare services and the insurance sector in order to preserve a tamper-proof record of data access. This feature is expected to facilitate early detection of unauthorized activities and thereby diminish the illegal profit gained through information leakage. On the other hand, numerous blockchain systems incorporate anonymity or pseudo-anonymity in transaction handling, potentially introducing an additional vulnerability. This section proposes a theoretical model that employs game theory to incorporate this aspect of anonymity.

Exemplification Scenario

Consider a large hospital radiology department pro- cessing several hundred scans daily, with over ten technicians holding access privileges. If blockchain is introduced in this environment, the advantage of indelible access logs can be offset by the dilemma posed by full anonymity, which makes it more challenging to identify precisely who viewed or removed data.

Model Overview

This framework focuses on the interplay between Leakage Risk Holder (e.g., healthcare professionals or insiders) who handle medical data and the Supervisory Entity (e.g., healthcare institutions, insurers, or regulators) that oversees the entire data management system. If the person at risk of causing a leak exploits blockchain's anonymity, they incur certain anonymity costs but may reduce the likelihood of detection.

Player Actions

Player A (Leakage Risk Holder)

i. **Action 1:** Violation (illicit data acquisition)

ii. **Action 2:** No Violation (no wrongful access)

Player B (Supervisory Entity)

i. **Action 1:** Monitor (enhanced oversight)

ii. **Action 2:** Relax (weakened surveillance)

In addition, let ϑ ($0 \le \vartheta \le 1$) denote the degree of anonymity provided by the blockchain system. A higher value of ϑ implies stronger anonymity. For example, $\vartheta = 0$ implies no anonymity (practically real name management), whereas $\vartheta = 1$ represents fully anonymized transactions.

Anonymity Risk and Detection Probability

Detection Probability Based on Anonymity

Although tampering with blockchain transactions is generally more difficult, higher anonymity can exacerbate the challenge of identifying who performed a given transaction. Let us define the probability of detection as

$$p_d(\vartheta) = p_o.(1-\alpha\vartheta),$$

where

i. p_0 is the baseline detection probability assuming tamper-proof logging on the blockchain (i.e., at $\vartheta = 0$).

ii. α is a parameter ($0 \le \alpha \le 1$) indicating the reduction in detection probability associated with an increase in anonymity.

iii. As ϑ rises, $(1 - \alpha\vartheta)$ decreases, causing $p_d(\vartheta)$ to become smaller.

Anonymity Cost

We also assume that Player A incurs costs to maintain higher anonymity on the blockchain (e.g., expenses related to specialized anonymization methods or mixing services). Let $C(\vartheta)$ capture these expenditures, growing monotonically with ϑ. For instance,

$$C(\vartheta) = c_0.\vartheta^{\beta}, \quad c_0 > 0, \beta \ge 1.$$

Here, $\beta \ge 1$ allows for accelerated cost growth as ϑ increases, modelling the potentially exponential expense of achieving greater anonymity.

Payoff Structures

Payoff for Player A (Leakage-Risk Holder)

If Player A chooses Violation, the expected payoff can be written as

$$U_A(Violation, \vartheta) = T - C(\vartheta) - p_d(\vartheta).S$$

where

i. T is the immediate gain from acquiring and reselling data (Temptation payoff).

ii. $C(\vartheta)$ is the cost of anonymity as discussed above.

iii. S is the penalty imposed if discovered (e.g., legal or disciplinary consequences).

iv. $p_d(\vartheta)$ is the probability that the illegal access is detected.

If Player A opts for No Violation, we set the payoff to be zero (or a small safe payoff R). For simplicity, we take it as zero:.

Payoff for Player B (Supervisory Entity)

When the Supervisory Entity (e.g., a hospital or regulatory body) chooses Monitor, it bears a certain oversight cost but can mitigate social losses by identifying breaches. We adopt a simple representation:

$$U_B(Monitor, \vartheta) = -K + p_d(\vartheta).\Delta,$$

where

i. K is the cost of continuous surveillance.

ii. Δ is the value added to Player B for successfully detecting a violation and thereby averting social harm (or receiving some form of recognition for successful detection).

iii. $p_d(\vartheta)$ applies only if Player A commits a violation.

If the Supervisory Entity selects Relax, the oversight cost is avoided, but no detection occurs. For simplicity, we set that payoff to 0:

$$U_B(\mathrm{Re}lax, \vartheta) = 0.$$

Example Computations

Player A's Optimal Strategy

Player A decides whether to choose Violation or No Violation based on:

$U_A(Vio., \vartheta) = T - C(\vartheta) - p_d(\vartheta).S$ vs. $U_A(No\ vio., \vartheta) = 0$ =tween

Player A will violate if:.

If anonymity ϑ can be selected (e.g., by choosing a particular anonymization tool), Player A will look for

Player B's Optimal Strategy

Meanwhile, the Supervisory Entity (Player B) chooses between Monitor and Relax. Since Player A's decision to violate or comply influences the outcome, Player B considers its expected payoff. If A violates, then monitoring yields

$$U_B(Monitor, \vartheta) = -K + p_d(\vartheta).\Delta.$$

If A refrains from violation, detection probability does not come into play, and Player B 's payoff for monitoring is effectively −K. By contrast, if B opts to relax, it avoids K but any violation remains undetected, resulting in zero payoff in our simplified model.

Suppose we set:

$T = 10$, $S = 20$, $p_0 = 0.8$, $\alpha = 0.5$,

$c_0 = 2$, $\beta = 2$, $K = 5$, $\Delta = 15$.

Hence, Player A's utility if violating is:

$$U_A(Violation, \vartheta) = 10 - (2\,\vartheta^2) - [0.8.(1 - 0.5\vartheta)].20$$

$$U_A(No\ Violation, \vartheta) = 0$$

and $p_d(\vartheta) = 0.8\,(1 - 0.5\vartheta)$.

Solving

$$\max_{\vartheta \in [0,1]} \{10 - 2\vartheta^2 - 0.8.(1 - 0.5\vartheta).20\}$$

Yields the anonymity level ϑ^* that maximizes Player A's expected return. Once ϑ^* is determined, Player B can predict whether A will commit a violation, and from there decide between Monitor and Relax accordingly. This simplified model mathematically shows that while blockchain can impede data tampering, strong anonymity features can simultaneously lower detection probability, introducing additional threats. In a healthcare/insurance joint platform, the interplay between "technical deterrence" (tamper-proof logs) and anonymity cost influences both partie's payoff's.

If Player A finds it profitable to commit data leakage while enjoying high anonymity, the Supervisory Entity may need to maintain constant monitoring to avert more frequent breaches. Yet if the monitoring cost K is too high, the incentive for B to choose Monitor diminishes, ultimately leading to Relax. Consequently, non-game-theoretic engineering and regulatory strategies— such as restricting the degree of anonymity, binding user IDs more rigorously to access logs, or setting sufficiently high penalties S so that illegal actions become unprofitable—are critical.

While *Kshetri* [19] highlights successful cases of blockchain implementations that offer robust resistance to tampering, the anonymity aspect may also generate opportunities for malefactors. The equations proposed in this research note articulate a trade-off, where higher anonymity ϑ decreases detection probability $p_d(\vartheta)$ but increases the cost $C(\vartheta)$. This balance can be analyzed through a game-theoretic lens.

Simulating a Nash Equilibrium in the Blockchain Model

This code shows an attempt to use game theory to examine the trade-offs between anonymity and penalty design when applying blockchain to sensitive fields such as medical data. It defines possible strategies for Player A (potential violator) and Player B (supervisory authority), discretizes the parameter space, determines each player's best response, and identifies any points that could serve as Nash equilibria.

Below, we describe the code's structure, the corresponding mathematical definitions, and how to interpret the resulting graphs. The "blockchain model" considered here can maintain high

anonymity and tamper-resilience, but may lead to complicated monitoring and cost scenarios.

Basic Model and Parameter Setup

Players and Strategies

a) Player A: Decide whether to commit a Violation or not to violate.

b) Player B: Decide to Monitor or to Relax.

Player A may gain payoff T through wrongful data acquisition but faces both anonymity costs and sanctions if discovered. On the other hand, Player B must spend resources to monitor, and in return can detect violations, reducing social losses.

Anonymity and Detection Probability

In the code, a parameter ϑ ($0 \le \vartheta \le 1$) denotes the degree of anonymity in the blockchain. A higher ϑ makes detection more difficult, although B's choice of Monitor (with cost K') might influence the overall detection rate. The code integrates ϑ with ϕ (representing the effect of multi-signatures or similar security measures) to finalize the effective detection probability, which then factors into each payoff function.

Example Parameters and Equations

At the beginning of the code, the following variables are defined:

a) $T = 15$: Primary gain from committing a violation.

b) $S = 15$: Punitive or social penalties.

c) $F = 10$: Additional penalty that could be enforced automatically (e.g., smart-contract-based deposit forfeiture).

d) $p_0 = 0.9$: Baseline detection probability without anonymity.

e) $\alpha = 0.6$: Rate at which higher anonymity reduces detection likelihood.

f) $c_0 = 3.0$, $\beta = 2.0$, $\lambda = 1.5$, $\gamma = 2.0$: Constants and exponents governing anonymity related costs.

g) $K' = 8.0$: Monitoring cost for Player B.

h) $\Delta = 20.0$: Social harm avoided by detecting a violation (interpreted as B's benefit).

i) $\Omega(\phi) = 2\,\phi^2$: Additional cost for stronger multi- signature mechanisms or organizational overhead.

Key formulas used in the code are summarized below:

i. Anonymity Cost

$$c(\vartheta,\phi) = c_0\ \vartheta^{\beta}(1+\lambda\phi^{\gamma}),$$

ii. Detection Probability

$$p_d(\vartheta,\phi) = p_0[1-\alpha\vartheta(1-\phi)],$$

iii. A 's Payoff (Violation)

$$U_A(Violate,\vartheta,\phi) = T - C(\vartheta,\phi) - p_d\ (\vartheta,\phi).(S+F),$$

iv. B 's Payoff (Monitor)

$$U_B(Monitor,\vartheta,\phi) = -K' + p_d(\vartheta,\phi).\Delta - \Omega(\phi)$$

Logic

Search via Discrete Grid

In the code, both ϑ and ϕ are divided into 51 points within the interval [0, 1], after which the algorithm exhaustively determines the optimal actions for Player A and Player B at each grid point. The results are stored in two-dimensional arrays:

1. A best action[i,j]: Denotes whether Player A chooses "Violate (1)" or "No Violation (0)".
2. B best action[i,j]: Indicates whether Player B selects "Monitor (1)" or "Relax (0)".

Nash Equilibrium Determination

A Nash equilibrium is defined as a point at which no player finds it profitable to unilaterally deviate, given the other player 's strategy. In the code, a simplified procedure is adopted to check for such equilibrium points:

1. First, for each (ϑ, ϕ), compute A best action [I, j] and B best action [i, j].
2. Next, determine whether the chosen strategy pair is mutually stable: that is, if neither player would change their own choice when presuming the other 's action is fixed.
3. If stability is confirmed, set NE array [i, j] = 1, marking a Nash equilibrium at that point; otherwise, set it to 0.

Trade-offs Between Anonymity and Suppression Features

Inspection of the outcomes suggests that in regions where ϑ (the anonymity parameter) is large, Player A's payoff for choosing Violation tends to increase, while detection probabilities tend to decrease. Consequently, A's inclination toward "Violate (1)" can prevail there. Meanwhile, as ϕ (level of multi-signature or access control) grows, the design makes high anonymity less effective. As a result, A's overall gain may decline.

Balancing B 's Monitoring Expense and Detection Gains

When Player B opts to Monitor, it must bear the cost K', and its benefits may further diminish if the term Ω(ϕ) (representing management overhead) also increases. Thus, if A is likely to choose No Violation, B may find that selecting Relax yields a higher utility. On the corresponding heatmap, one can observe the boundary region distinguishing B's "Monitor" choice from its "Relax" policy.

Observing Nash Equilibrium Points

Where the heatmap (i.e., NE array) indicates a value of 1, both A and B do not alter their respective strategies (checked on a discrete

grid). In practice, there may be territories in which A's best choice is "No Violation" and B's best choice is "Relax." Conversely, a different zone might favor A 's "Violate" and B 's "Monitor." The equilibrium conditions are shaped by the interplay of $\mathcal{G}$ and ϕ, balanced against detection likelihoods and cost constraints.

Although simplified, this code can serve as an exploratory method for using game theory to assess the trade-off between anonymity and monitoring costs in blockchain systems intended for highly confidential data—such as in medical or insurance contexts [19,11].

Significance

1) Provides a foundational framework for modelling advanced blockchain implementations (including ZKPs, multi-signatures, homomorphic encryption) [21,28].

2) By analysing the distribution of Nash equilibria and payoffs for both players, it is possible to evaluate how introducing anonymity influences deterrence of misconduct.

Limitations

1) Future research would benefit from parameter calibration using real-world data from healthcare or insurance industries, incorporating more realistic costs, detection probabilities, and penalty designs.

2) Potential extensions include continuous optimization or stochastic approaches (e.g., evolutionary games) to consider dynamic strategic shifts over time [5].

Issues Requiring Attention by the Analyst

Although the code applies a game-theoretic perspective to examine risk and cost—treated as parameters like anonymity or monitoring expenditure—when leveraging blockchain technology in areas such as healthcare or insurance, it remains necessary to acknowledge various constraints arising from simplifications and parameter assumptions, as well as broader sociotechnical aspects. Below is a concise summary of the principal factors demanding particular vigilance.

Challenges and Considerations

Validity of Parameter Settings

Many of the parameters adopted in this model (e.g., anonymity degree $\mathcal{G}$, suppression coefficient ϕ, detection probability p_0, and anonymity cost c_0) can be difficult to estimate in real life scenarios. For instance, measured data regarding insider misconduct in hospitals and the actual costs of anonymity-enhancing technologies are typically limited or highly variable across different organizations. Thus, analysts should:

a) Base parameter ranges on literature reviews and direct interviews to reflect real-world conditions as closely as possible.

b) Conduct sensitivity analyses to see how equilibrium outcomes fluctuate with variations in parameter values, checking the robustness of conclusions.

Treatment of Detection Probability and Simplified Modelling

In the code, detection probability is largely modelled in a binary manner: if B monitors, there is a certain detection rate; otherwise, it is effectively zero. However, real blockchain systems may permit partial or graded detection. Furthermore, the monitoring cost and detection probability could be interlinked, with additional resources producing higher detection efficacy. Analysts should:

a) Consider multilevel monitoring models (e.g., higher cost yielding higher detection, intermediate cost with moderate detection, etc.).

b) Incorporate empirical data and operational reports to refine the detection function so that it better reflects continuous real world behaviour.

Accounting for Social and Political Factors

Misconduct involving personal health data or insurance information often arises within a legal, political, and organizational context not easily translated into numerical form. Even if simulations hint at an equilibrium solution, organizational culture or stakeholder conflicts may prevent implementation of that theoretical optimum [2]. Analysts should:

a) Combine qualitative analysis (e.g., interviews and case studies on internal controls and work- place culture) to validate the assumptions of the quantitative model.

b) Investigate policy incentives, external regulations, and industry norms—factors not reflected in the baseline model—and include them in supplemental scenarios.

Payoff Structures and Adapting to Multidimensional Contexts

This code adopts a simplified payoff design: Player A's benefit is largely monetary, while Player B's advantage is tied to avoiding a social loss. In reality, healthcare professionals might be motivated by reputational factors, internal evaluations, or intangible benefits. Analysts should:

a) Consider multidimensional utility functions that include not only monetary payoffs but also factors like reputation, trust, and emotional elements.

b) Introduce alternative or proxy variables to better represent real human decision-making in the payoff formulation.

Scalability and Computational Cost

Currently, the code uses an exhaustive search over 51×51 points for $\mathcal{G}$ and ϕ. This approach is still tractable for a two-dimensional parameter space but would become exponentially more expensive for additional dimensions or finer mesh sizes. Analysts should:

a) Employ computational optimizations (e.g., adjusting grid resolution, using parallel computing) to ensure feasibility for more extensive explorations.

b) Integrate advanced optimization methods (e.g., gradient-based or evolutionary algorithms) to handle large-scale parameter spaces and more intricate payoff functions.

Ethical and Privacy Challenges

Analyses involving real data on medical or insurance records must mitigate privacy threats and comply with personal information regulations. It is essential to clarify the legitimate scope of data usage and implement robust anonymization. Additionally, in blockchain- based systems, granting excessive access privileges to sensitive data must be avoided. Design choices should address these concerns to safeguard patient and client confidentiality.

Overall, this game-theoretic approach, as demonstrated by the code, is potentially valuable for exploring the trade-off between anonymity and deterrence in highly secure environments such as healthcare data platforms or insurance frameworks. Nonetheless, numerous caveats demand attention—particularly regarding parameter uncertainty, social contexts, and model simplifications. Since multiple stakeholders are involved in healthcare ecosystems and organizational norms are often complex, integrating quantitative models with qualitative assessments is strongly recommended.

Test Results: Discussion and Comparison of Outcomes Under Various Parameter Adjustments

(Figure 1-3)

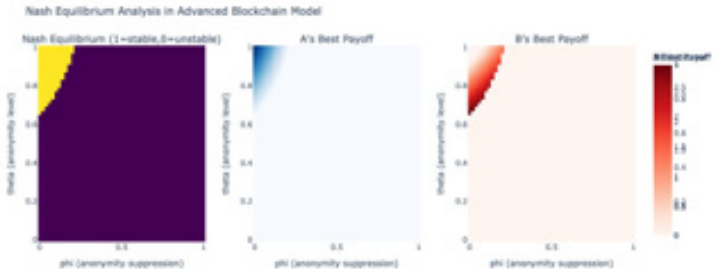

Figure 1: Nash Equilibrium Analysis in Advanced Blockchain Model (1).

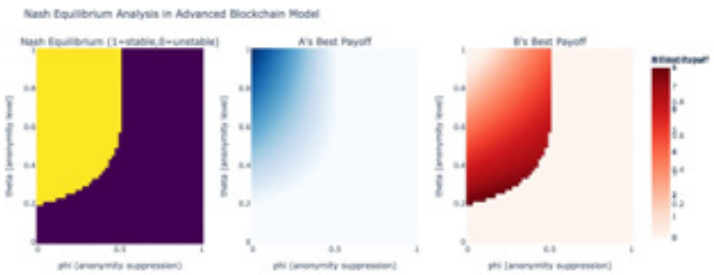

Figure 2: Nash Equilibrium Analysis in Advanced Blockchain Model (2).

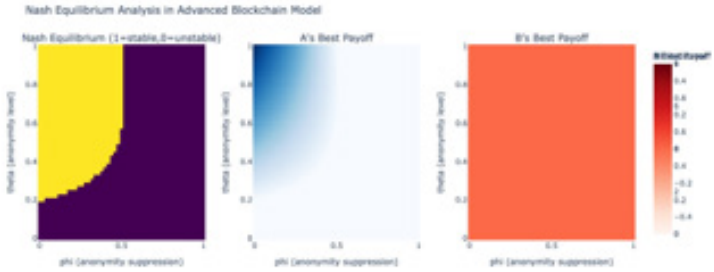

Figure 3: Nash Equilibrium Analysis in Advanced Blockchain Model (3).

Analysis of Nash Equilibria and Best Payoffs for Players A and B under Varied Parameters

The figures are three heatmaps generated by running the same code while modifying parameters. From left to right, they represent:

i. Map displaying whether a Nash equilibrium is stable or not (1 = stable, 0 = unstable),

ii. Map showing Player A's best payoff, (Figure 4)

iii. Map showing Player B's best payoff.

In these simulations, we vary several parameters (for instance, T representing Violation profit, K′ corresponding to monitoring costs, and α denoting the rate at which detection probability declines) and compare how the stability region and distribution of best payoffs change accordingly.

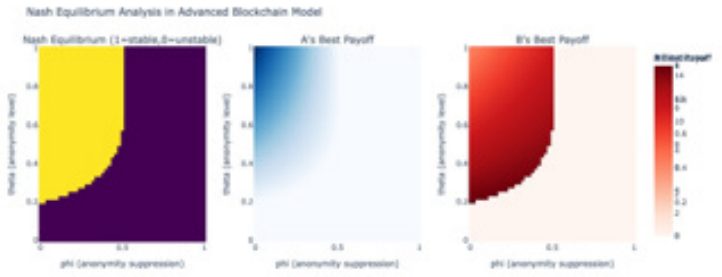

Figure 4: Nash Equilibrium Analysis in Advanced Blockchain Model (4).

Shifts in the Nash Equilibrium Distribution

Left figure: A map that indicates points of Nash equilibrium (yellow = 1) versus points of no equilibrium (purple = 0). Altering the parameters may expand or contract the yellow region or shift thresholds along the $\mathcal{G}$ or ϕ axes.

Generally, higher $\mathcal{G}$ (anonymity) makes it more likely for Player A to select "Violation," whereas higher ϕ (multi-signature or access control strength) raises detection probability and therefore incentivizes Player B to choose "Monitor. "Depending on the parameters, however, B' s monitoring costs or management burdens might grow, creating zones of instability.

A wide expanse of yellow suggests that within a specific range of $\mathcal{G}$ and ϕ, both players 'best responses coincide frequently. Conversely, a map dominated by purple might imply that A's and B's interests diverge so that stable points are scarce, or that in large portions of the parameter space A consistently chooses Violation and B cannot effectively counter it due to cost constraints.

Player A's Best Payoff (Center Figure)

This visualization displays the payoff Player A receives after comparing "Violation" against "No Violation" and selecting whichever yields the higher utility. Darker shading indicates higher payoff for A over the ($\mathcal{G}$, ϕ) plane.

Typically, greater $\mathcal{G}$ enhances anonymity, making it easier for A to exploit the payoff T. Yet, when ϕ is large, detection probability grows and additional expenses (e.g., from multi-signatures) may accumulate. How these influences are parameterized affects the colour distribution in the middle figure.

Comparing the plots, one might observe that in upper regions (i.e., large $\mathcal{G}$) the colour can deepen (e.g., more intense blue), reflecting A's growing payoff. On the other hand, as ϕ increases to moderate or high levels, that payoff may drop because of heightened detection likelihood, causing lighter colours.

Player B's Best Payoff (Right Figure)

The right figure shows Player B's payoff after comparing "Monitor' 'with "Relax," where darker (reddish) shading denotes higher payoff for B.

For B, higher detection probability (achieved by large ϕ or small $\mathcal{G}$) can more readily curb misconduct, but surveillance cost and Ω(ϕ) can erode B's net returns. Moreover, increasing the parameter K' (monitoring expense) can reduce B's advantage from monitoring, potentially making "Relax" more profitable over wide regions.

When parameters vary, one may observe scenarios in which only a restricted band of ϕ and $\mathcal{G}$ produce bright red (high payoff), or alternatively the entire area appears muted (lower payoff). These disparities stem from whether B's cost burden is modest or steep, as well as from the assigned value of detection benefits Δ.

Overall Comparison across Parameter Adjustments

a) Nash equilibrium diagram (left): Significant changes in this map typically arise from major shifts in K' (B's monitoring cost), Δ (benefits from detection), or T (A's illicit gain). If monitoring becomes prohibitively expensive, B is less inclined to monitor, allowing A to violate more readily. This scenario can move the equilibrium region.

b) A's best payoff diagram (center): Increasing T makes violation more lucrative for A, heightening payoffs in high-$\mathcal{G}$ regions. However, if detection probability or penalty levels are

also increased, A's net payoff even under high anonymity may be diminished.

c) **B 's best payoff diagram (right):** Monitoring cost K' and avoided loss Δ are pivotal. Low K' and large Δ enlarge the area in which monitoring yields high payoffs (deep red colour). Conversely, if K' is high, B might opt for Relax over a wide range, leading to a generally lower payoff landscape.

Comprehensive Observations

Alterations in each parameter affect whether A capitalizes on anonymity, whether B can afford rigorous monitoring, or whether both fall back on more cautious strategies. These dynamics in turn reshape the stable Nash equilibrium zone in the left figure.

When the yellow region in the left figure expands, it indicates more combinations of $\mathcal{G}$ and ϕ align with both players' equilibrium strategies. For instance, if B's monitoring cost is contained and detection benefits are high, B tends to monitor, and A foresees this and refrains from violating, thus broadening stable solutions.

Conversely, a narrow yellow region suggests only a limited set of strategies simultaneously satisfies both A and B. In certain parameter ranges, A might frequently elect to violate while B is deterred from monitoring due to costs, creating a pronounced mismatch.

Middle (A's payoff) and right (B's payoff) plots show their "tug of war." Extreme values of anonymity or multi-signature constraints ($\mathcal{G}$ or ϕ) might reward one side greatly at the other's expense. Such cases often prove unstable, corresponding to purple (unstable) domains on the left map.

Conclusion

Comparing graphs obtained by changing multiple parameters confirms that the region of stable Nash equilibria is highly sensitive to factors such as monitoring cost, violation payoff, and penalty level. Furthermore, how the payoffs for Player A (the offender) and Player B (the supervisory entity) balance each other depends heavily on the configuration of anonymity ($\mathcal{G}$) and multi-signature suppression (ϕ). If anonymity is extensive, A's gains rise, but outcomes also hinge on B's ability to handle its monitoring expenses; this dynamic can destabilize equilibrium or shift to alternative stable strategy pairs.

These simulation results show, in a framework reminiscent of a prisoner's dilemma or Stackelberg game, the parameter domains in which a socially desirable deterrent situation becomes feasible. Researchers and system designers can refer to such maps when deliberating cost sharing, penalty intensification, or the optimization of anonymity settings. Further parameter specific investigations will be presented in the next research note.

Additional Risks and Concerns When Using Offensive Measures or Strong Sanctions Before Suspects are Clearly Identified

Past analyses of data leakage risks in healthcare organizations and of misconduct presuppose an environment where the suspect is at least partly identified when applying simulations or designing sanctions. In reality, implementing aggressive measures or severe penalties before a suspect is unambiguously identified can spawn new threats and adverse consequences. This includes expanding the scope of potential targets, thereby amplifying risk, and imposing penalties or warnings on unrelated individuals who are not even direct stakeholders. This section discusses such supplementary risks from an alternative vantage point.

Loss of Public Confidence and Avoidance of Healthcare Services

If a medical institution, as part of suspect-tracking, broadens the scope of logs or extends monitoring beyond staff and patients to unrelated third parties, it may spark societal anxiety. From the viewpoint of patients and local residents, the impression that "the hospital is gathering extensive personal data under the guise of security or investigation'' can prompt them to avoid the facility altogether. Consequently, people may delay necessary medical services or screenings, escalating the hazards to public health.

Internal Control Turmoil and Organizational Conflict

Announcing the possibility of large-scale monitoring or harsh penalties to locate a suspect could disrupt internal control within a healthcare facility. Mutual distrust may emerge among personnel, and friction could escalate between managerial and frontline staff. If a pervasive sense of "we cannot trust anyone regarding information leaks'' takes hold, communication will deteriorate, undermining the quality of clinical care. Moreover, whistleblowing programs intended to expose wrongdoing might degenerate into "informant battles," eroding both institutional safety and order.

The Paradox of Security Enhancement and an Expanded Attack Surface

When suspects remain unknown, swiftly reinforcing security often entails tightening defensive measures on every communication channel and device, requiring system overhauls and renegotiated contracts with providers. This complexity can introduce fresh vulnerabilities and configuration errors. In effect, "offensive measures for defense'' risk dispersing attackers and potential rogue insiders across a broader frontier, unwittingly enlarging the scope of what they can target. As the infrastructure becomes more convoluted, oversight may fail to keep pace, undermining efficient protection of medical data.

Confusion in Cross Organizational Data Sharing

Healthcare providers increasingly manage not only patient records but also data linked to partner pharmacies and insurers. If search or sanction measures are conducted before identifying the suspect, a large volume of information might be shared across organizational boundaries. Where the delineation of the hospital 's domain is imprecise and data from unrelated entities is also scrutinized or exposed, tensions can escalate widely. In a hospital group operating internationally, there is the added danger of breaching overseas data protection laws.

Potential for Collective Bias and Discrimination

Absent a clearly identified suspect, biases or conjectures could arise—for instance, regarding certain nationalities, ethnicities, or professional groups—leading to speculation about who poses a higher risk of leaking data. Such attitudes can foster discrimination in medical environments, affecting patient intake and hiring. If such sentiment intensifies, it may result in the wrongful exclusion of persons or denial of care, aggravating the risk of harm for innocent parties.

The Danger of Re-Spreading Fake News

As previously discussed, investigative or surveillance actions initiated before a suspect is identified risk being amplified by social media or news outlets. Local communities and patients can be misled by unreliable stories, fueling rumors and inaccurate claims about particular medical organizations or staff. The public health impact could be especially detrimental if, for instance, incorrect information about an infectious disease response spreads, stirring up vaccine hesitancy or reluctance to seek care, thus heightening adverse health outcomes.

Implications for Unrelated Third Parties and Legal Liabilities

Attacking or sanctioning people when the suspect has not been firmly pinpointed may fail to mitigate leakage risks; paradoxically, it may broaden them. Unrelated individuals could be implicated, raising legal liabilities and eroding internal stability, while promoting bias or prejudice that extends beyond the institution. In other words, while it may appear to be an act of "expedient justice" to "attack others alongside the suspect," the secondary losses and burdens must be carefully weighed. Ultimately, misguided investigations and aggressive surveillance in medical settings under- mine patient care quality, degrade institutional credibility, and potentially further leakage, misinformation, and public-health drawbacks. Hence, an exceedingly cautious approach is essential.

Addressing Clusters Affected by Misinformation and the Necessity of Their Care

Previous discussions have highlighted the legal and ethical risks that emerge if healthcare-related wrong- doing occurs and the paradox wherein applying strong surveillance or sanctions prematurely may actually amplify confusion or data breaches. In reality, even when suspicion is misplaced, there is a high probability of forming clusters of individuals caught up collectively through misinformation. Once stigmatized as suspects, they suffer social and psychological harm and may in turn avoid seeking medical attention. Consequently, follow-up and care for such clusters become indispensable.

Clusters Incited by Misinformation

When a false allegation or rumor circulates—e.g., "Hospital XYZ is experiencing a massive security breach," "All insiders are presumably culpable" —the result could be a wave of condemnation encompassing staff or patients who have no real involvement. Entire ethnic or professional subgroups might be lumped together and targeted, creating a severe psychological burden. Victims may hesitate to consult healthcare providers about their own medical issues, for fear of further stigmatization.

Exploitation by Impostors Pretending to be Suffering Clusters

A further complication arises if malicious actors masquerade as victims supposedly harmed by suspicion or prejudice. For instance, a group might claim "we are being unjustly accused," while actually persisting in insider data theft or collaborating with external criminals to steal medical records. By portraying themselves as injured parties, they can potentially dissuade authorities from monitoring them or solicit external sympathy, thereby circumventing compliance protocols.

The Right of Healthcare Providers, Families, and Patients to a Safe Environment

Even amidst misinformation and involvement of innocent parties, medical organizations have a duty to ensure an environment where patients, families, and healthcare personnel can participate in or receive care with confidence in a clean setting. Although a certain degree of suspicion may be unavoidable, excessively aggressive tactics should be tempered by:

a) **Protecting Privacy and Dignity:** Conducting broad surveillance on uncertain suspects could severely violate the privacy of innocent individuals.

b) **Sustaining Continuity of Medical Services:** Suspicion arising from rumors or investigations should not deter patients from seeking care nor compromise staff cooperation.

c) **Minimizing Mental Stress for Families and Stakeholders:** Prevent lump sum accusations against family members, and establish guidelines for explanation and follow-up.

Considerations within this Research Project

This research (and related simulations) emphasize the following:

1) **Controlling Cluster Formation via Misinformation:** When employing dynamic game theory or adopting blockchain, it is vital to anticipate incorrect allegations and rumor propagation. One must design procedures enabling circumscribed, step-by-step monitoring alongside protection for whistleblowers, offering consistent accountability to individuals presumed to be suspects in order to forestall unwarranted clustering.

2) **Dialogue and Support Protocols for Affected Groups:** Providing follow-up and psychological assistance for those erroneously monitored or suspected is essential. Collaborations with medical social workers or counsellors can help gather feedback from individuals who felt unfairly accused or fear losing their jobs due to suspicion.

3) **Transparency in Organizational Measures and Education:** Medical staff must be trained to understand that misguided investigations or group profiling can degrade patient care. Especially when cooperating with external entities (insurance

companies or law enforcement), explicit guidelines are needed to clarify how much data is disclosed and how stakeholders' rights are upheld.

4) **Gradual Simulation and Practical Validation:** From a research standpoint, running multi-period game-theoretic models with varying parameters can reveal how overly harsh sanctions and monitoring might exacerbate "misinformation led clustering.'' For actual pilot implementations, it is prudent to start with smaller-scale clinics and then expand coverage incrementally.

Emphasizing a Careful Perspective

Addressing clusters swept up by unfounded rumors is an often-overlooked dimension of safeguarding confidentiality in medical contexts. Undue intensification of sanctions when suspects remain unidentified can lead to secondary harm for misidentified groups, who might then forgo healthcare or psychological support. If impostors or fake news also enter the mix, hospital trustworthiness and public health outcomes could plummet. Although this research applies blockchain technology and dynamic game theory to design deterrence against misconduct, protocols must incorporate strategies to curtail misinformation-based clustering and provide care for those wrongly implicated, as well as follow-up mechanisms for whistleblowers or misidentified individuals. Ensuring that healthcare practitioners, patients, and families can practice and receive care in a clean, secure environment demands both technical and organizational-cultural approaches.

Nash Equilibrium Analyses from the Same Code under Varied Parameters, and an Additional Viewpoint on Clusters Driven by Misinformation: The Role of Media

This section focuses on Nash equilibrium analyses derived from executing the same code with different parameter values, as well as the best payoffs (Best Payoff) for each of Players A and B. These are presented as three heatmaps. Next, we discuss how clusters—formed under the influence of misleading information —can create multi-layered repercussions that go beyond mere erroneous accusations. In particular, we address viewpoints not previously discussed, emphasizing the complexity of caring for clusters coerced by misinformation.

Amplification through Social Media Communities

When misinformation proliferates on social media, individuals initially disinterested in healthcare matters may become engaged, resulting in collective backlash or the recreation of false claims. If an SNS community coalesces, a large number of users can quickly label the "target hospital" or "suspicious staff " as culpable, sometimes even implicating unrelated patients or family members. As group polarization escalates, it grows increasingly difficult for mistakenly stigmatized clusters to voice their perspective at all.

Secondary Harm from Mass Media Coverage

If false information on a healthcare dispute garners widespread media attention, secondary harms risk be- coming magnified. For instance, a tabloid show or news program might sensationally cover the "hospital under suspicion," inadvertently tainting all staff with a negative image. Consequently, vague but pervasive fears— "the entire staff is unsafe," "no one should go there" —can permeate the public, expanding the cluster of unfairly condemned individuals.

Segregation in the Information Sphere and Barriers to Care

Once discourse fractures between those believing misinformation and those holding accurate data, certain clusters may begin eschewing healthcare services entirely. For example, if an online community becomes convinced that "everyone working in that facility is colluding in wrongdoing," patients who genuinely need care may instead receive repeated messages reinforcing distrust, making them even less likely to seek medical treatment. In these segmented spaces, it becomes almost impossible for healthcare professionals to pro- vide corrective information. As a result, the barriers to accessing care dramatically increase.

Caution Regarding Further Impersonators

Among individuals recognized as requiring help due to misinformation, opportunistic criminals may feign

the identity of aggrieved parties to gain internal access or collect intimidation materials in collaboration with external perpetrators. In other words, "attackers disguised as victims" can manipulate the hospital's inclination to assist, for example by persuading it to reveal sensitive data or ease auditing procedures. Consequently, the institution must maintain robust per- mission management and logging practices even while offering aid.

Care Perspective: Psychological Support and Rectifying Misinformation

Care for clusters wrongfully accused or engulfed by rumors must address:

a) **Psychological Assistance:** Setting up resources such as counseling and third-party committees for staff or patients who were unfairly targeted.

b) **Public Correction of Misinformation:** Promptly issuing official statements clarifying the facts, along with corrections if allegations prove baseless. Disseminating accurate information in collaboration with relevant parties before rumors propagate too far.

c) **Reconfirming Protections for Service Users:** Even when coordinating with external entities, strictly avoid oversharing personal data to minimize the formation of "misinformation clusters."

Although medical settings must ensure that staff, patients, and families can work and receive treatment in a clean and safe environment, situations in which misinformation spawns a new victimized cluster often go unaddressed. Although this research (or simulation model) integrates dynamic game theory and blockchain to examine optimal sanctions and surveillance intensities for illicit actors, we

must incorporate the perspective of caring for clusters harmed by misinformation. Future work must explore the academic modelling of how to provide compensation, psychological help, and processes to correct misinformation for such misidentified groups or those harmed by rumors. This approach can enhance not only the deterrence of wrongdoing but also strengthen social trust and re-assurance for both patients and healthcare staff.

Care for clusters inadvertently caught up in misinformation is frequently overlooked in efforts to reduce data leak risks in healthcare, yet it is vital to protect organizational credibility and public well-being. Particularly when malicious parties disguise themselves

As "victims needing support," opportunities for infiltration and wrongdoing multiply, complicating remediation. Consequently, hospitals should moderate aggressive surveillance before identifying suspects, while also establishing a system to offer immediate and appropriate care should innocent individuals be misidentified. Drawing on these insights, this research will explore expansions to dynamic game models, methods for mitigating misinformation-driven clusters, and strategies for preserving the rights of healthcare employees, patients, and families to engage in medicine with confidence.

Clusters Caught by Misinformation and the Need for Their Care

Information leaks and erroneous accusations of misconduct have long been subjects of considerable concern in the healthcare environment. However, beyond immediate discussion lies an additional dimension in which misinformation prompts the formation of clusters unconnected to the real suspect, imposing substantial psychosocial pressures on those involved. This situation underscores the necessity for deeper approaches to "care" in response to misinformed groups. Below, we present supplementary insights not previously covered.

Linkages to Dark Markets or External Forums on the Internet

When misinformation or fake news about health care spreads, the source and resonance points may extend beyond local hospitals or communities. The internet hosts various dark markets and anonymous forums where rumors can be deliberately amplified or tweaked, fostering the creation of misinformation clusters. As false "reports of harm" accumulate in these external spaces, the illusion may arise that the institution in question imposes broad-scale vigilance or penalties, thus fueling distrust among outsiders. Ultimately, individuals may refrain from accessing medical services, aggravating public health consequences.

Novel Fraud and Solicitation Preying on "Clusters in Need of Care"

Misinformed clusters—individuals under psychological strain or socially isolated—are vulnerable targets for con artists posing as medical professionals, peddling expensive products, or recruiting for illegal activities. Exploiting the institution 's "safe space" narrative, they may promise "we can rescue you," thereby obtaining personal information for illicit purposes. Without centralized oversight by hospitals or municipal services, these vulnerable clusters remain unguarded against unscrupulous organizations.

Global Infodemic Countermeasures

The phenomenon of misinformation induced condemnation toward healthcare institutions or personnel can become an international concern. In particular, misinformation regarding infectious diseases and public health can cross borders, forcing cooperation among numerous hospitals and international agencies. If these rumors catch fire in foreign SNS platforms or communities, it becomes unclear how to deliver care or track evolving scenarios, heightening complexity. The lack of robust international collaboration can inadvertently amplify medical distrust worldwide.

Stakeholder Conflicts Concerning Care Provision

Determining how to offer assistance to misinformed clusters typically involves multiple parties: hospitals, insurers, governmental agencies, patient advocacy groups, etc. Their interests may clash—for example, "providing aid or info to unconnected individuals increases cost," or "strict screening is required to avoid mixing suspects and true victims." Resulting delays can cause extended or worsened harm for these clusters.

Cultural and Linguistic Hurdles in Providing Care

Cultural and linguistic differences substantially affect both how misinformation spreads and how it is interpreted. In certain areas, medical professionals wield high authority, making fake news less likely, while in others, persistent healthcare skepticism can foster easy acceptance of rumors. In multilingual environments, translation delays or unintentional misinterpretations may hamper efforts to disseminate accurate information. Hence, care systems in multicultural, multilingual contexts must address these nuances.

Efforts to Remain Alert Without Overreacting— The Present Work 's Approach

Healthcare institutions must preserve an environment in which staff, patients, and families can safely work and receive treatment. Complementing vigilance against impersonation or further misconduct, the following measures are critical:

1) **Addressing Cultural and Linguistic Diversity:** When language barriers fuel misinformation, or clusters emerge in diverse cultural settings, hospitals must provide trustworthy, multilingual resources. Partnering with interpreters and other specialists can curtail rumors and ensure that everyone with a genuine need can access assistance.

2) **International Cooperation and Academic Networks:** Given the global scale of rumor mongering, international networks of medical institutions and researchers are essential. Shared standards and protocols can expedite the introduction of best practices in caring for misinformation clusters and reduce the harm of disinformation.

3) **Permanent Psychological Support Services**: Among those who distrust the hospital may be individuals in dire need of medical help. Hence, it is crucial to include social workers or clinical psychologists on the team to provide specialized care for those grappling with suspicion or trauma.

4) **Digital Literacy and Risk Communication:** Beyond dynamic game theory and blockchain-based security, public literacy campaigns and risk communication are vital in an era of digital misinformation. If healthcare workers and patients possess basic awareness of rumor spreading pathways, they can mitigate harm more swiftly.

Previous analyses of healthcare information leakage risk often presumed that the entity committing misconduct (or seeking maximum profit from fraudulent behavior) was, to some extent, identifiable. However, in reality, attacks or sanctions can occur before the suspect is definitively identified, posing a recognized danger of heightened legal liabilities and further leakage risks [22,24]. Actions undertaken based on "some piece of evidence" can expand unwarranted suspicions to unrelated third parties, intensifying risk for external stakeholders and individuals entirely unconnected with the situation.

Uncertain suspect identification potentially impacts a broad set of stakeholders, including healthcare personnel, patients, insurers, and IT vendors [29,19]. If suspicions misdirect investigations and sanctions— coupled with expansive data gathering such as logs or personal information—these collected resources them- selves can leak. Hence, ironically, the very activities meant to catch the suspect might enlarge the circle of harm [11]. Issuing blanket alerts or penalties to a large group can undercut legitimate whistleblowing, spawn confusion, and potentially let the actual perpetrator evade detection.

Instances have been documented of organizations imposing strong sanctions or launching premature attacks when the suspect was unknown, and ultimately harming innocent people by violating their rights or tarnishing their reputations [2,24]. This fosters diminished morale, legal vulnerabilities, and even further obstructions to whistleblowing. To mitigate these perils, experts recommend gradual monitoring procedures before suspect confirmation and collaboration with external or third-party oversight mechanisms to minimize wrongful allegations. In a blockchain system with elevated anonymity, suspect identification may be even more difficult, thus amplifying these paradoxical problems. As anonymity heightens, pinpointing the real perpetrator becomes more challenging, but the scope of suspicion broadens. We aim to integrate such a paradox—where inadequate suspect identification can escalate data breach and legal dangers—into game-theoretic models and layered frameworks addressing organizational care methods, as well as strategies against misinformation clusters. It remains crucial to determine how to restrict penalties or notices that might inadvertently spill over to innocents, while balancing monitoring or whistle blowing systems.

Information leak prevention in healthcare has long been acknowledged as a pressing challenge, and adopting blockchain-based solutions has raised expectations of novel frameworks. Here, we concentrate on four dimensions in examining how medical misconduct or rumor driven harm can be analyzed over extended periods and from multiple perspectives:

a) **Incorporating Blockchain and Dynamic Game Theory:** Beyond single period (static) models that mainly consider short-term payoffs, multiperiod structures and multidimensional utility functions can assess the long run incentives of the offender (A) and the supervising body (B). We focus on how anonymity in a blockchain environment might suppress wrongdoing and how to optimally design surveillance or penalty costs.

b) **Emergence of "Aggression" from Misinformation, Social Turbulence, and Cluster Formation:** In healthcare, false accusations and rumor dissemination can harm unrelated staff or patients. Overreactions can paradoxically entrap those who are in fact innocent, complicating social confusion. We examine how to model these complexities in a dynamic game context.

c) **Dilemmas Involving Children and Younger Generations as Targets or Disseminators:** Contemporary research suggests that vulnerable children—sometimes the principal victims—can be pushed into spreading misinformation. This underscores the insufficiency of mere sanctions and surveillance in healthcare and demands consideration of younger cohorts as both possible spreaders and sufferers of falsehoods.

d) **Care Perspective and Organizational Responses:** When misinformation clusters arise, opportunistic fraud and retaliation become more likely. Thus, a multi-layered approach— extending beyond technology and including internal whistleblower protection, mental health sup- port, and digital literacy—is necessary. We explore embedding these care considerations into dynamic game models, thereby guiding institutional designs and procedures for equitable, safe healthcare.

In doing so, we articulate how blockchain and dynamic game theory add value to tackling data leak risks and misinformation in medical fields, while highlighting the urgency of embedding issues involving younger demographics and holistic care. We aim to integrate these insights into practical implementations and future research.

Paradox of Heightened Leakage Risks from Casting Suspicion on Third Parties

Until now, our research notes have primarily examined scenarios in which the perpetrator of misconduct (or the party seeking to maximize illicit gains) is relatively identifiable, facilitating game-theoretic simulations or penalty design. In real situations, however, it is risky to impose sanctions preemptively without solid identification, and excessive measures may ensnare un related parties. This can paradoxically increase data leakage hazards. Below, we discuss how uncertainty in identifying suspects can inflate

healthcare data vulnerabilities, and the mounting dangers of penalizing or issuing warnings to innocent individuals.

Legal Dangers of Sanctions Before Identifying the Suspect

Attempting to boost surveillance or punitive measures without pinpointing the real suspect may raise legal concerns about monitoring questionable individuals or related persons. For instance, monitoring someone based on IP addresses or login histories may overstep lawful investigative authority, ultimately constituting privacy violations or unwarranted investigation [22]. If a healthcare institution proceeds without official authorization, yet the suspect proves unrelated, the institution itself could face legal liability. Accordingly, incentives often favor postponing aggressive audits or sanctions until the suspect is confirmed.

Enlarged Suspicion and Frequent Alerts

To capitalize on "some piece of information" by conducting broad investigations can paradoxically expand the risk of data leakage. For instance, collecting every staff member's email's or system logs to isolate the wrongdoer also harvests personal information about uninvolved employees. If the monitoring system itself exhibits gaps, the logs and surveillance data can leak, compounding the breach potential [11].

Additionally, upon detection of misconduct, an organization might adopt blanket warnings or semi disciplinary notices targeting all staff (or a broad range of affiliates). Yet this can suppress legitimate whistle blowing and heighten external distrust. A disproportionate reaction penalizes innocent parties, stifles shared information, and inflates the organization 's overall risk exposure.

Penalty Risks for Unrelated Third Parties

When ramping up collaborative inquiries with outside entities—like insurers or regulatory agencies— healthcare organizations may inadvertently share data on individuals who are tangential or wholly unconnected [29]. In such cross organizational information exchanges, innocent parties may be mistakenly flagged and penalized (e.g., denial of insurance claims or calls to suspend services). Under HIPAA, for instance, improperly transferring irrelevant personal information can represent a double privacy infringement, exposing the institution to further legal complications.

Unique Uncertainties of Medical Settings and Organizational Culture

The interplay of patients, families, and staff frequently defies a simple "offender vs. institution" dynamic. In particular, suspect identification can be delayed by personal or familial ties, which may obscure the facts [2]. If hierarchical pressure or concealment arises, it becomes challenging for suspects to step forward or for witnesses to present evidence, leaving investigations futile. Bolstering sanctions in such an environment risks implicating innocent personnel and undermining healthcare service delivery.

Case Studies: Misdirected Probes and Involvement Risks

Bazerman and Tenbrunsel [24] describe how expanding suspicion across the organization can cause non-offenders to shrink back, thereby hindering genuine disclosures and delaying the discovery of the real culprit. Similarly, Japanese research on whistleblowing in healthcare [2] demonstrates how excessive mistrust fractures cooperative systems, ironically fostering concealment. Hence, a misconstrued suspect profile that broadens the scope of an investigation can produce a paradox by slowing down the apprehension of actual violators.

Proposed Responses and Means of Control

In addressing this issue, one could consider a multifaceted approach until the suspect is definitively established:

a) **Gradual Surveillance and Limited Data Collection:** Instead of monitoring everyone indiscriminately, concentrate on reasonably high probability suspects. Moreover, strictly separate permissions for any logs or access data and store them securely to prevent secondary leakage.

b) **Partnering with External Organizations:** Involve objective agencies for auditing and specialized investigations. Independent third parties can reduce the risk of penalizing non-culprits, as medical institutions alone may lack legal authority for such actions.

c) **Strengthening Internal Whistleblower Protection:** As indicated in previous work [24,2], developing a supportive institutional and cultural environment encourages tip offs from staff who sense wrongdoing. This can lessen the need for extensive, indiscriminate monitoring.

Increasing Risks Instituting robust sanctions or surveillance before the suspect is adequately identified can inadvertently compromise individuals beyond the genuine perpetrator, infringing on privacy and legal protections. Where confidential patient data is involved, these perils may be significantly heightened, producing organizational fear, suppressed whistleblowing, and further leaks. Consequently, a careful design of deterrence measures must account for suspect identification uncertainty, in tandem with external, neutral auditing and targeted surveillance—while reinforcing internal reporting systems. Taken together, these strategies enable more precise isolation of genuine criminals while limiting unwarranted penalties or leakage dangers, safeguarding fairness and security in medical facilities.

Risks of Capitalizing on "Certain Information" for Identifying Suspects and International Case Examples

In healthcare settings, prematurely implementing stringent sanctions or surveillance before a suspect is clearly identified not only poses legal risks but can also adversely affect unrelated individuals and outside parties. Indeed, legal infractions or severe penalties overseas may result from such actions. Additionally, from ethical and humanitarian standpoints, these measures raise serious issues and can facilitate the spread of fake news, ultimately harming public health.

Legal Liabilities and Overseas Penalties

Improper handling of medical records and personal data can potentially violate multiple legal frameworks, including privacy protection laws and criminal codes. For instance, under HIPAA (Health Insurance Portability and Accountability Act) in the United States, collecting or disclosing the data of unrelated third parties is considered a major violation, potentially leading to tens of thousands of dollars in fines or even imprisonment in cases deemed both intentional and malicious [29]. In the European Union, GDPR (General Data Protection Regulation) applies particularly stringent standards when dealing with medical data. If an institution or corporation engages in improper monitoring or data collection, it risks a penalty of up to 4% of its annual worldwide turnover or 20 million euros, whichever is higher [26].

These regulations clarify that even if the goal is to prevent data leakage or identify suspects, unjustified or excessive surveillance of uninvolved individuals cannot be legitimized. If a hospital exploits "certain information" to obtain extensive logs or conduct blanket monitoring—while inadvertently capturing third-party data in the process—it faces markedly elevated legal liability.

Ethical and Humanitarian Concerns

Investigative or punitive tactics under the banner of "suspect identification" may clash with the funda- mental ethics of healthcare, namely prioritizing patient dignity and continuity of care. For instance, broad searches of patient records performed by hospital staff—bypassing or minimizing internal whistleblowing— can breach patients' privacy and undercut the trust between healthcare professionals and patients. Moreover, if monitoring extends to unrelated families or external institutions, the willingness of stakeholders to cooperate with the hospital may fall, potentially lowering the caliber of collaborative care.

From a humanitarian perspective, overreaching investigations and sanctions for medical data controversies threaten patient autonomy and basic human rights, inflicting emotional distress on individuals unjustly suspected or accused. When a healthcare facility 's role in offering "secure and trustworthy care'' is twisted for policing or suspect elimination, it undermines the core principles of clinical practice.

Fake News Propagation and Impacts on Public Health

When threats or sanctions target those outside the actual suspect pool, misinformation can circulate among staff or within patient communities, potentially fueling fake news. This phenomenon misleads external stake- holders and unrelated parties alike, generating rumors such as "Hospital X is conducting a massive illicit investigation" or "All patient data has leaked.'' These narratives can spark reputational damage, prompting some individuals to avoid using essential healthcare services and thus elevating public health risks. For example, refusing or delaying treatment in response to rumors about an infection outbreak may inadvertently promote its spread throughout a region.

Indeed, there have been documented instances in which intense media coverage of a medical mishap or misconduct negatively affected vaccination rates in a locality, as well as cases in which incorrect health information was amplified exponentially over social media [31]. Should an inquiry into medical data breaches be mismanaged—leading to unrestrained data collection or the casting of unfounded suspicions— further health hazards and diminished healthcare access become increasingly plausible.

Public Health Risks and the Dilemma of Issuing Warnings

Launching excessive surveillance or imposing severe sanctions prematurely often calls for large-scale public alerts, potentially convincing the healthcare work force, patients, families, and local communities alike that "some form of wrongdoing is underway.'' On one hand, it may appear beneficial for transparency, but on the other, it imposes emotional burdens on those not actually implicated and adds to staff workload. It can also, as noted, accelerate the dissemination of fake news, posing a paradoxical challenge. Inadequate communication risks failing to curb further harm, while excessive warning generates needless panic, ultimately hindering public health operations and disrupting the proper use of medical resources.

Exploiting "certain information" to identify a suspect—and in turn taking action against others beyond the suspect—can thus escalate additional dangers from legal, ethical, and humanitarian angles, while also giving rise to fake news and broader public health set backs. As shown by overseas examples such as HIPAA and GDPR, comprehensive monitoring or breaches of data belonging to uninvolved individuals can lead to substantial fines or criminal liability. Furthermore, from a humanitarian standpoint, mistakenly collecting or labeling third parties' data as suspicious constitutes an outright violation of fundamental rights. Factoring in the societal costs of fueling fake news or undermining public health strongly suggests that large- scale audits or punitive actions must be approached with extreme caution at the preidentification stage. Instead, limiting and phasing data handling, cooperating with neutral external bodies, and strengthening internal reporting mechanisms provide alternative paths. These steps can prevent unwarranted investigations and penalties against innocent parties and preserve the main mission of healthcare.

Additional Hazards and Concerns Stemming from Attacks and Sanctions Before Suspect Identification

Analyses of healthcare information leaks and misconduct have generally been premised on the assumption that "the suspect is at least partially identified.'' Yet, in practice, forcibly or prematurely issuing sanctions before definitive suspect identification can generate fresh risks and adverse outcomes. Not only might the scope of targeted individuals expand—thus magnifying data leakage risks—but observers have also noted that unrelated parties or external stakeholders may be subjected to warnings and penalties. Here,

from a supplementary viewpoint, we discuss further possible dangers stemming from such scenarios.

Erosion of Institutional Credibility and Reluctance to Seek Care

When a healthcare institution undertakes large-scale log retrieval or surveillance—possibly extending beyond patients and staff—the public may become profoundly unsettled. From the perspective of patients and local residents, the impression may form that "the hospital is amassing vast amounts of personal data under the pretense of security or investigations," potentially deterring individuals from seeking care. As a result, more people may forgo necessary medical exams or treatments, heightening the public health risks.

Disruption of Internal Control and Organizational Conflict

Threats of extensive oversight and rigorous sanctions can unsettle the entire governance structure of a medical facility. It may engender mutual suspicion among employees and damage rapport between management and the general workforce. If staff cannot ascertain who might be responsible for breaches, the environment can devolve, obstructing information sharing and undermining the quality of clinical collaboration. Moreover, whistleblower systems may instead create "mutual denunciation" within the organization, destabilizing institutional order and safety.

The Paradox of Enhanced Security and Expanding Attack Surfaces

In the absence of a concrete suspect, rushing to strengthen security implies adopting defensive measures across all channels and devices, requiring extensive system modifications and revised contracts with service providers. This can render systems more complex, introducing fresh vulnerabilities and configuration mistakes. The so-called "offensive approach to defense" can inadvertently scatter potential malicious insiders or hackers even further, effectively expanding the scope of what they can target. As a system grows more intricate, it becomes increasingly difficult to manage and monitor, potentially lowering the efficiency of data protection.

Chaos in Data Sharing Beyond Organizational Boundaries

Healthcare facilities are increasingly storing not just patient data but also records from affiliated pharmacies and insurance companies. If punitive action or investigative measures continue without a definite suspect, voluminous data might be shared across organizational boundaries. Ambiguities can arise about which tasks belong explicitly to a healthcare setting, and personal data from unrelated organizations might be brought under scrutiny or inadvertently exposed. In hospital groups spanning multiple countries, the risk of violating foreign data protection laws further complicates matters.

Group Bias and the Promotion of Discrimination

When the suspect remains unidentified, speculation may swell regarding certain nationalities, ethnic back- grounds, or occupational groups, labelling them as "highly likely to be responsible for leaks." Such stereotyping can foster discrimination and bias in healthcare, influencing patient interactions and hiring processes. As suspicions intensify, those wholly uninvolved could be unwarrantedly excluded, or denied proper medical attention.

Renewed Warning about the Dissemination of Fake News

As previously discussed, investigations or monitoring commenced before confirming the suspect might be exaggerated through SNS or media outlets. If the local community or patient base becomes swayed by unverified information, false narratives may take root regarding an entire facility or consortium, undermining public health. Specifically, if accurate data is vital during an infectious disease outbreak, but rumors gain traction first, vaccine hesitancy or refusal of care could ensue, amplifying possible harm.

Attacks or sanctions undertaken without clear suspect identification form a paradox: rather than mitigating healthcare data leakage, they can expand it in myriad ways. Innocent third parties, legal exposures, organizational disarray, prejudice, and the spread of misinformation may extend the problem beyond any single facility. In other words, while it might be viewed as a straightforward act of "carrying out justice" to pursue individuals beyond the main suspect based on "some information," the secondary repercussions and dam- age must be soberly assessed. Ultimately, flawed investigations or augmented surveillance in clinical settings can degrade patient care and institutional credibility, while intensifying information leaks, erroneous reporting, and public health detriments—making restraint and diligence indispensable.

Children and Younger Demographics in Misinformation Clusters: Harm to Victims and Patterns of Dissemination

Thus far, we have shown that misinformation can spur excessive surveillance or punitive actions in healthcare, dragging innocent groups into an expanding cycle of negative impact. Recent studies, however, point to an alarming development: children of ten emerge as principal victims of misinformation. Furthermore, it appears that students and young adults such as freelancers are significantly involved in circulating these inaccuracies. Below, we take these additional points into account to explore misinformation clusters in healthcare more deeply.

Why Children Become Targets of Misinformation

In the healthcare sector, children's inadequate self defence capabilities and limited media literacy are said to render them the earliest potential victims of misinformation [32]. For instance, when rumors or falsehoods about vaccines or illnesses spread on social networks, children—and their parents—may be- come anxious and avoid vital services. Moreover, children can face bullying or discrimination based on mis- perceptions, especially if synergy between schools and healthcare providers is weak, causing interventions to lag behind. Internationally, there have been reports of anonymized or partially redacted health records in- tended for school submissions being posted online, giving thousands of forum visitors access to the private information of a child or an entire class. Such episodes not only jeopardize that child's privacy but also

incite speculation that "all classmates have some illness," prompting harassment or truancy.

Students and Freelancers as Disseminators of Misinformation

Recent research suggests that among those actively propagating or reproducing untrue claims or slander about hospitals and medical staff, students and young freelancers stand out [33]. This demographic can quickly forge a sense of unity on internet forums, occasionally running hashtag campaigns aimed at certain medical facilities. Commonly, such individuals have no direct involvement but are motivated by self- expression or the desire for recognition, making it difficult to stabilize the situation. For instance, hashtags such as "#Dangerous Hospital" or "#Fraudulen- tRecords" might trend among students who post sensational allegations as a form of entertainment, with large volumes of unverified material accumulating in a short timeframe. Some participants may exaggerate or fabricate details purely to draw attention, posing a grave threat to trust in the hospital or its employees.

The Risk to Children and Limiting Access to Medical Data

When children are collateral damage in misinformation, drastic reductions in their medical access can ensue. For example, a widely circulated false claim that a particular hospital is experiencing an outbreak could deter parents from taking their children for necessary shots or check-ups [31]. Such an avoidance response, predicated on inaccuracies, not only compromises the region's collective public health but also potentially inflicts irreparable harm on the children affected.

Addressing Youthful Spreaders: Digital Literacy and Social Incentives

In analyzing why students or freelancers emerge as primary conduits for false allegations, experts note that the low psychological barrier and sense of belonging found in online networks are central drivers [33,34]. Sharing or amplifying provocative claims about hospitals or healthcare staff can rapidly garner attention, yielding social validation for participants. As a result, effective strategies for reducing misinformation in medical contexts must consider these social incentives and incorporate digital literacy programs and awareness campaigns for young demographics.

Practical Care: Approaches for Both Children and Disseminators

Where misinformation clusters revolve around children, healthcare institutions should focus on:

a) **Child-Friendly Information Delivery:** Favor approachable, visually oriented resources over technical medical jargon or statistical data.

b) **Coordination with Parents and Schools:** Collaborate with educational bodies and local communities to facilitate rumor fact checking and consistent sharing of accurate medical updates.

c) **Encouraging "Constructive Dissemination" among Young People:** Shift students and freelancers away from posting misinformation toward redistributing expert opinions or factual medical data (e.g., by adopting group-based fact-checking on social media).

Research Scope: Dynamic Game Theory and Misinformation Clusters

While the present research (or simulation model) examines the suppression of wrongdoing through dynamic game theory in combination with blockchain, protecting vulnerable groups, such as children, and addressing the actions of young spreaders require more than mere sanctions or oversight. When misinformation circulates, it becomes pivotal to incorporate into the dynamic model how to care for clusters involving children and how to guide young disseminators toward credible information rather than punishing them. In doing so, healthcare organizations can theoretically develop a multifaceted approach that safeguards the rights of families, workers, and patients while breaking the chain of disinformation.

In sum, healthcare misinformation clusters take on greater urgency when children are especially susceptible as victims or prime targets. Moreover, as indicated by studies highlighting the role of students and freelancers in rumor propagation [32,33], straight forward sanctions alone are inadequate—digital literacy and community engagement strategies provide crucial buffering. Practically, protecting children while positively redirecting youthful disseminators demands coordinated involvement from medical institutions, educators, governments, and more. Hence, to expand this game-theoretic model, researchers must address "misinformation dynamics," "care for harmed clusters," and "motivations behind its spread" to balance safety in healthcare with the preservation of public health. Our subsequent discussion envisions such a model and deliberates on its implications.

The Game-Theoretic Model Presented in this Paper and the Challenges of Blockchain Utilization

The game theory model and blockchain utilization framework presented in this paper is only an initial exploratory study, and further empirical research and verification of field implementation are needed. Specifically, the following points are considered to be the main issues to be addressed in the future.

a) **Refinement of Parameter Estimation:** Quantitative data on anonymity costs and penalty settings need to be obtained and reflected in the model, based on leakage cases that have occurred at actual medical institutions and the terms of contracts with cloud contractors.

b) **Implementation of Multi Period Models and Evolutionary Approaches:** The analysis can be made more realistic by considering the dynamics of healthcare institutions changing their strategies over the long term and evolutionary game models that include the learning effects of external attackers.

c) **Development of Specific Operational Guidelines:** When implementing a blockchain-based medical information man-

agement system, comprehensive operational guidelines are needed on how to link patient handling, staff training, and third-party audit processes.

d) **Approach to Cultural and Social Aspects:** No matter how optimized the technology and penalties are, if there is a lack of consideration for sociocultural factors such as whistleblower protection, organizational climate, and fake news measures, the effectiveness of the system may be significantly reduced. Multidisciplinary research that takes these factors into account is desirable.

Based on the above issues, we would like to establish safer and more feasible countermeasures against the third-party via risks faced by Japanese medical practices through continuous research, development, and demonstration.

In Closing

This study emphasizes that its discussion of health- care data leakage risks within Japan does not seek to criticize healthcare professionals. Rather, what we wish to highlight most is the increasingly severe reality of external third parties leaking data and the structural factors behind this phenomenon. While blockchain's tamper-resistance and anonymity can, if operated properly, help protect patient privacy and enhance transparency in auditing, one must remain aware of the risk that excessive anonymity may allow insiders or external attackers to slip by undetected. By applying a game-theoretic model, we have gained guidelines on how to configure sanctions or monitoring costs to maximize deterrence against wrongdoing, as well as on how to assess trade-offs involving anonymity costs.

On the other hand, issues surrounding information management in healthcare settings involve a complicated array of stakeholders, including not only healthcare personnel and organizational culture but also patients, insurance cooperatives, and IT vendors, all influencing one another. The examination of Japanese case examples presented in this paper constitutes an initial exploratory consideration, focusing on the risk of third-party leakages and strategies for prevention. In future work, we must refine model parameters by drawing on empirical data and compare these findings with international data protection regulations, thereby seeking a security management system well-suited for actual medical practice.

Ultimately, it is vital for domestic healthcare institutions to prioritize preventing "third-party related data leaks" by comprehensively revisiting technical upgrades, training, legal frameworks, and organizational structures. We hope that such endeavors will elevate the reliability and privacy safeguards of medical services in Japan, fostering an environment in which every stakeholder, including patients, can securely use healthcare services.

Acknowledgments

This study was written after reviewing the Life Science Ethics Checkpoints, Personal Information about People and Data Ethics. We would like to express our deepest gratitude to the many physicians and other concerned individuals who provided guidance and advice for this study, as well as to the local medical institutions that have supported our family on a daily basis. The author has also been in possession of some diseases for a long time and continues to receive treatment. In particular, I would like to express my gratitude to the many doctors, pharmacists, and other medical professionals who have been involved in psychiatric treatment over a long period of time. I would also like to thank the LLM developers for their efforts and all their wisdom.

Conflict of Interest

None.

References

1. (2018) Japan Network Security Association, Survey Results on Information Security Incidents: Personal Information Leaks.
2. Takemura Y (2019) Barriers to Internal Whistleblowing in Japanese Nursing Organizations: A Qualitative Approach. Journal of Nursing Studies 12(2): 56-67.
3. (2025) Information Technology Promotion Agency, Japan (IPA), Survey on Information Security Incidents Caused by Internal Fraud.
4. Zyskind Guy, Nathan Oz, Pentland Alex Sandy (2015) Decentralizing Privacy: Using Blockchain to Protect Personal Data, In 2015 IEEE Security and Privacy Work shops, IEEE: 180-184.
5. Fudenberg Drew, Maskin, Eric (1986) The Folk Theorem in Repeated Games with Discounting or with Incomplete Information. Econometrica 54(3): 533-554.
6. Morley Jessica, Floridi Luciano, Kinsey Laura, Elhalal Anat (2020) From GDPR to COVID- 19: Infra Ethics, Shadow Nudges, and Incomplete Regulatory Tools. BMJ Health & Care Informatics 27(3): e100123.
7. Bates David W, Sheikh Aziz (2016) The Future of Health Information Technology in the Patient-Centered Medical Home, The American Journal of Managed Care 22(3): 225-227.
8. Thaler Richard H, Sunstein Cass R (2008) Nudge: Improving Decisions About Health, Wealth, and Happiness, Yale University Press.
9. Nat Zone (2024) What is HIPAA and Its Impact on Japan.
10. Maxwell Thomas, Richardson Benjamin (2019) Information Health and Patient Outcomes: A Multi Hospital Analysis. Health Informatics Review 4(3): 23-39.
11. Sicari S, Rizzardi A, Grieco LA, Coen Porisini A (2015) Security, Privacy, and Trust in Internet of Things: The Road Ahead. Computer Networks 76: 146-164.
12. (2025) Information Technology Promotion Agency, Japan (IPA), Survey on Information Security Measures in SMEs-Case Studies.
13. (2019) House of Representatives of Japan, The 198th Diet, Cabinet Committee, No. 15.
14. Anderson R (2006) Security Engineering: A Guide to Building Dependable Distributed Systems (2nd Edition), Wiley.
15. Weick Karl E, Sutcliffe Kathleen M (2007) Managing the Unexpected: Resilient Performance in an Age of Uncertainty (2nd ed.) Jossey- Bass.
16. Narayanan Arvind, Bonneau Joseph, Felten Edward W, Miller Andrew, Goldfeder Steven (2016) Bitcoin and Cryptocurrency Technologies, Princeton University Press.
17. Azaria Asaph, Ekblaw Ariel, Vieira Thiago, Lippman Andrew (2016) MedRec: Using Blockchain for Medical Data Access and Permission

Management, In 2016 2nd International Conference on Open and Big Data (OBD), IEEE: pp. 25-30.

18. (2024) HIPAA Journal, HIPAA Violation Cases.
19. Kshetri Nir (2017) Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy, Telecommunications Policy, 41(10): 1027-1038.
20. Tirole Jean (1988) The Theory of Industrial Organization, MIT Press.
21. Ben Sasson, Eli Chiesa, Alessandro Garman, Christina Green, Matthew Miers, et al., (2014) Decentralized Anonymous Payments from Bitcoin, In 2014 IEEE Symposium on Security and Privacy, IEEE: 459-474.
22. Anderson Ross J (2008) Security Engineering: A Guide to Building Dependable Distributed Systems (2nd Edition), Wiley.
23. Borgatti Stephen P, Everett Martin G, Freeman Linton C (2002) UCINET for Windows: Software for Social Network Analysis, Analytic Technologies.
24. Bazerman Max H, Tenbrunsel Ann E (2011) Blind Spots: Why We Fail to Do What's Right and What to Do About It, Princeton University Press.
25. (2025) National Police Agency of Japan, Risk Assessment Report on Crime Proceeds.
26. (2018) PwC Japan Group, GDPR Penalties: Examples of Violations and Considerations for Penalty Decisions.
27. Bonneau Joseph, Miller Andrew, Clark Jeremy, Narayanan Arvind, Kroll Joshua A, et al., (2015) SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, In 2015 IEEE Symposium on Security and Privacy, IEEE: 104-121.
28. Gentry Craig (2009) A Fully Homomorphic Encryption Scheme, Ph.D. Thesis, Stanford University.
29. Stylemap (2024) Complete HIPAA Guide: Data Security Requirements and Compliance Tips.
30. Ostrom Elinor (1990) Governing the Commons: The Evolution of Institutions for Collective Action, Cambridge University Press.
31. (2020) World Health Organization, Managing the COVID-19 Infodemic: Promoting Healthy Behaviors and Mitigating the Harm from Misinformation and Disinformation.
32. Livingstone S (2009) Children and the Internet: Great Expectations, Challenging Realities, Polity Press.
33. Bartlett J, Miller C (2011) Truth, Lies, and the Internet: A Report into Young People's Digital Fluency, Demos.
34. Buterin Vitalik (2018) Sharding FAQ.