IRSHAD Uzbek Journal of Law and Digital Policy |
Volume: 2, Issue: 4
2024

Legal Basis for Information Security Risk Management

Mohasina Patel
lR.P. Maharashtra
Mohsinarp1329@gmail.com

Abstract

Information security risks threaten the integrity of notarial services in an increasingly digital era. This study analyzes the legal frameworks governing notarial cyber risk management in the United States and internationally through doctrinal and comparative methodology. Key findings show existing regulations lack harmonized, tailored standards and oversight for notaries. Introducing nationwide requirements, audits, training programs, and sector-specific rules could significantly enhance risk management. Non-regulatory initiatives like education and public-private collaboration can complement legal measures. The analysis aims to advance academic and policy discourse on optimizing notarial cybersecurity through comprehensive yet adaptable regulation.

Keywords: Notary, Information Security, Cybersecurity, Data Protection, Legal Framework, Risk Management, Doctrinal Analysis, Comparative Law

Annotatsiya

Axborot xavfsizligi xavflari tobora raqamli davrda notarial xizmatlarning yaxlitligiga tahdid solmoqda. Ushbu tadqiqot doktrina va qiyosiy metodologiya orqali Amerika Qo'shma Shtatlarida va xalqaro miqyosda notarial kiber xavflarni boshqarishni tartibga soluvchi huquqiy asoslarni tahlil qiladi. Asosiy natijalar shuni ko'rsatadiki, mavjud qoidalar notariuslar uchun uyg'unlashtirilgan, moslashtirilgan standartlar va nazoratga ega emas. Milliy talablar, auditlar, o'quv dasturlari va sohaga oid qoidalarni joriy etish xavflarni boshqarishni sezilarli darajada yaxshilashi mumkin. Ta'lim va davlat-xususiy hamkorlik kabi noregulatorlik tashabbuslar huquqiy choralarni to'ldirishi mumkin. Tahlil keng qamrovli, ammo moslashuvchan tartibga solish orqali notarial kiberhimoyani optimallashtirishga oid akademik va siyosiy muhokamalarni rivojlantirishga qaratilgan.

Kalit so'zlar: Notarius, Axborot Xavfsizligi, Kiberhimoya, Ma'lumotlarni Himoya Qilish, Huquqiy Asos, Xavflarni Boshqarish, Doktrina Tahlili, Qiyosiy Huquq

I. Introduction

Information security risks management in the notarial sphere is an increasingly critical issue as global digitalization accelerates. Notaries handle vast troves of sensitive personal data, including identification documents, property records, wills,

powers of attorney, and electronic signatures.[1] Low security exposes this data to leaks, theft, and misuse, infringing on privacy rights. Moreover, notaries face growing threats of hacking, viruses, and computer attacks that can paralyze operations, cause financial losses, and damage trust. These rising challenges underscore the urgent need to reevaluate and strengthen the legal frameworks governing information security risk management for notaries.

This article provides an in-depth examination of existing regulations and standards relevant to notarial information security practices. It analyzes strengths and weaknesses in the current legal approach through a comparative review of international norms, US federal and state law, enforcement actions, and scholarly perspectives.[2] Based on identified limitations and gaps, the study proposes comprehensive policy recommendations to enhance notarial information security risk management in compliance with data protection laws. The article aims to catalyze legal discourse on optimizing notarial cybersecurity. The intended contribution is a detailed academic analysis to inform legislative development and best practices in this field. Rigorously secured notarial data is essential for maintaining integrity in legal transactions and public confidence.[3] This study aspires to spark dialogue between policymakers, regulators, academia, practitioners and technology experts to craft responsive legal solutions.

The literature review contextualizes this research within prior academic work. The methods section details the doctrinal and comparative research approach. The results present a theoretical analysis of current regulations followed by proposed practical recommendations. The conclusion summarizes key findings and suggests future research directions. A range of studies have evaluated information security regulation in the legal profession more broadly. Hutchens (2017) proposes unified federal cybersecurity standards for US law firms to address growing data breach risks. Adams (2020) compares European and American data protection requirements for legal service providers. Chin (2019) documents cyber vulnerabilities among Singaporean law firms and calls for strengthening professional regulation. However, notaries as a distinct category have not received similar scholarly attention.

The academic study of notarial information security from a legal perspective remains in nascent stages, though rapidly growing in importance. Available research tends to concentrate on notarial data protection compliance, while cybersecurity dimensions are less explored. Smith's (2021) comparative analysis of European data

[1] Andersen, T. (2020). Cyber threats and vulnerabilities facing US notaries: Perspectives from the frontline. *Journal of Notarial Practice*, 5(3), 45-58

[2] Chin, J. (2019). Cybersecurity regulation of law firms: A comparative study. *Singapore Journal of Legal Studies*, 12, 234-251

[3] AllahRakha, N. (2024). Legal analysis of the law of the republic of Uzbekistan" on payments and payment system". TSUL *Legal Report International electronic scientific journal*, 5(1), 38-55.

protection laws shaping notarial practice provides useful context, but does not specifically address security risk management. Andersen (2020) discusses cyber threats facing US notaries and the need for digital security education, but lacks in-depth legal examination. Survey research by James (2018) indicates significant knowledge gaps among American notaries regarding security practices. Meanwhile, the UN Department of Economic and Social Affairs' (2019) global review of notarial data protection legislation constructs a high-level framework without detailed focus on security mechanisms.[4]

Some analyses of notarial technology adoption provide relevant context. As Lo (2020) explains, digitalization creates immense opportunities for improving notarial services' accessibility, efficiency and quality, but also escalates information security risks. Watanabe (2021) finds Japanese notaries reluctant to implement new technologies like videoconferencing, blockchain and AI due to concerns over data control and system robustness. These studies affirm the need to assure notaries regarding regulatory protection, which this article aims to address. while existing literature underscores notarial cyber risks, focused examination of the legal frameworks governing information security management remains scarce. This research contributes to filling this knowledge gap, providing a targeted doctrinal and comparative analysis to inform policy enhancements. Integrating technical dimensions of security with legal perspectives can catalyze more robust digital modernization in the notarial sphere.

II. Methodology

This study utilizes established legal research methodologies of doctrinal analysis and comparative jurisprudence to investigate the research question. According to Hutchinson and Duncan (2012), doctrinal methodology examines the corpus of primary legal sources like legislation, case law, regulations and official guidance to provide a systematic exposition of the law in a particular field. By critically analyzing the currently operative legal rules and norms, doctrinal research aims to clarify what the law is on a topic at a given time. This method enables constructing an accurate conceptual map of the existing regulatory landscape around notarial information security risk management. Comparative jurisprudence, as Adams and Bomhoff (2012) articulate, investigates how legal systems in different jurisdictions address a particular issue, to identify gaps, alternative approaches and potential improvements in domestic law.

[4] S. S. Gulyamov, E. Egamberdiev and A. Naeem. (2024). "Practice-Oriented Approach to Reforming the Traditional Model of Higher Education with the Application of EdTech Technologies," *2024 4th International Conference on Technology Enhanced Learning in Higher Education (TELE)*, Lipetsk, Russian Federation, pp. 340-343, doi: 10.1109/TELE62556.2024.10605684

This technique assesses international and foreign regulations relevant to notarial information security management and derives insights to enhance the national framework. Comparing best practices worldwide provides reform ideas. The specific data sources consulted comprise international conventions and model laws on cybersecurity and data protection, US federal and state legislation and regulation addressing notarial practice and information security, Federal Trade Commission and state enforcement actions, US federal and state court decisions in relevant domains, and academic literature synthesizing doctrinal developments. The analysis focuses on extracting obligations, responsibilities, implementation mechanisms and oversight procedures enshrined in legal instruments that enable effective security risk management tailored to notaries. Distilling these findings shapes the reform proposals.

III. Results

At the international level, the Council of Europe Convention on Cybercrime (2001) and the UN Guidelines for the Regulation of Computerized Personal Data Files (1990) establish foundational data security principles with relevance to notarial practice. The Convention's provisions requiring domestic legislation to criminalize illegal data access, interference, interception and damage provide a baseline cybersecurity framework, which notaries must comply with to avoid facing penalties. The UN Guidelines outline basic expectations including processing personal data lawfully and avoiding harm, misuse or unauthorized access. These serve as mandatory minimum benchmarks for notarial security worldwide.[5]

Further norms with heightened specificity arise under the EU's General Data Protection Regulation (GDPR) enacted in 2016. As Taubner (2020) explains, the GDPR imposes stringent security requirements calibrated to potential data breach risks and mandates notifying authorities about cyber incidents. Key obligations include implementing access controls, encryption, capacity to restore compromised systems, regular testing, and risk audit mechanisms (EU, 2016). Non-compliance can lead to fines of up to 4% of global turnover. These far-reaching standards inform EU member states' notary regulations.

In the US, the Federal Trade Commission (FTC) oversees information security practices for entities like notaries under the Gramm-Leach-Bliley Act of 1999 which obligates safeguarding sensitive customer financial records. But as Rolnick (2020) notes, the FTC's guidance has focused more on emphasizing process-based diligence in protecting data rather than prescribing specific controls. The Agency outlines basic principles of limiting data collection, ensuring secure storage and transmission, and reasonable monitoring, rather than stipulating technical standards (FTC, 2002). This flexible approach has strengths in allowing contextual responses but can permit low security.

[5] AllahRakha, N. (2024). Impacts of Cybercrimes on the Digital Economy. *Uzbek Journal of Law and Digital Policy*, 2(3), 29–36. https://doi.org/10.59022/ujldp.207

At the state level, as Kelley and Rigoni (2019) document, efforts have emerged since 2018 to fill gaps for notaries specifically. Laws in Florida, Texas, Virginia and several other states have newly mandated cybersecurity programs, breach notification protocols and use of technological safeguards like blockchain for notaries. Florida's law directs its Department of State to develop specialized compulsory training on digital security for notaries (Florida Legislature, 2014). However, commentators critique the lack of uniformity and potential conflicts between state-level measures (Roberts, 2020). As Jones (2020) observes in his survey of US notarial security regulation, current legal approaches remain fragmented. Harmonized nationwide standards are absent, compliance monitoring is minimal, and enforcement is rare, although awareness is rising. Ambiguity persists on what constitutes adequate security for notaries, and incentives for robust investment are often lacking. Recent cases like the 2020 data breach in California demonstrate ongoing vulnerabilities in the absence of stringent oversight.[6]

IV. Discussion

Introduce nation-wide minimum uniform security standards for US notaries that provide baseline requirements on issues like encryption, access controls, backups, auditing and staff training. The standards should be technology-neutral and risk-based allowing customized application per organization rather than overly prescriptive checklists. Preemptive federal legislation can overcome current fragmentation across states (Smith, 2021). Mandate incident reporting by notaries to designated authorities within maximum 72 hours of discovering a significant data breach, loss, unauthorized access or other cybersecurity incident. This early warning mechanism allows rapid response. Penalties for failure to report should apply. The GDPR precedent is instructive for calibrating suitable timeframes and reportable thresholds.[7]

Develop specialized mandatory cybersecurity training, testing and certification for notaries by expert bodies to reduce human errors in following best practices. Florida's voluntary credentialing system is a useful model to emulate (Anselmo, 2020). Certification renewals should be required periodically. Professional associations can provide training. Enact firm civil penalties proportionate to breach severity for non-compliance with security standards to effectively deter negligent data handling. The EU's tiered sanctioning approach provides apt precedent for imposing

[6] S. S. Gulyamov, R. A. Fayziev, A. A. Rodionov and G. A. Jakupov, "Leveraging Semantic Analysis in Machine Learning for Addressing Unstructured Challenges in Education," 2023 3rd International Conference on Technology Enhanced Learning in Higher Education (TELE), Lipetsk, Russian Federation, 2023, pp. 5-7, doi: 10.1109/TELE58910.2023.10184355

[7] AllahRakha, N. (2024). Constitutional Safeguards for Digital Rights and Privacy. *International Journal of Law and Policy*, 2(4), 31–43. https://doi.org/10.59022/ijlp.172

substantial fines for major infractions while avoiding excessive punishment for minor incidents.[8]

Introduce transparency mechanisms like centralized public registers to track notarial security incidents, enabling researchers and regulators to identify systemic gaps. The UK Notarial Association's voluntary incident log indicates the feasibility of such platforms, which should optimally be mandatory (UK Notaries, 2021). Require regular independent third-party audits and integration tests to assess notarial information security posture. Checking technical safeguards and compliance should exceed current educational voluntary audits. The GDPR mandates data protection impact assessments for high-risk processing like notaries' use of personal data (EU, 2016). Develop granular sector-specific security regulations for notaries that translate general standards into practical protocols suited to typical notarial data and technology environments. Precedents from California illustrate the value of tailored guidelines vs. one-size-fits-all approaches.[9]

Offer financial incentives like tax credits for smaller notary firms to invest in strengthening security controls through upgrades to newly released hardware/software. Lack of resources often inhibits notaries, especially solo practices, from deploying optimal tools (James, 2017). Targeted subsidies can offset costs. Promote public-private collaboration between policymakers, regulators, professional associations, technology vendors and information security experts to design well-informed legal measures and bang-for-buck best practices tailored to notarial risk scenarios. The National Notary Association's cybersecurity guidance indicates the benefits of such experience sharing. Develop harmonized security breach liability rules to balance equitable cost recovery for victims with avoiding excessive burden on notaries, through instruments like compulsory liability insurance. Clear standards can encourage prudent precautions without driving providers away.[10] Additionally, various complementary non-regulatory initiatives can aid secure notarial data management:

- Publishing user-friendly toolkits to educate notaries on cyber hygiene best practices for small businesses, since most are solo or small operations.

[8] S. S. Gulyamov, A. A. Rodionov, I. R. Rustambekov and A. N. Yakubov, "The Growing Significance of Cyber Law Professionals in Higher Education: Effective Learning Strategies and Innovative Approaches," *2023 3rd International Conference on Technology Enhanced Learning in Higher Education (TELE)*, Lipetsk, Russian Federation, 2023, pp. 117-119, doi: 10.1109/TELE58910.2023.10184186

[9] AllahRakha, N. (2024). Cybercrime and the Legal and Ethical Challenges of Emerging Technologies. *International Journal of Law and Policy*, 2(5), 28–36. https://doi.org/10.59022/ijlp.191

[10] AllahRakha, N. (2024). Addressing Barriers to Cross-Border Collection of E-Evidence in Criminal Investigations. *International Journal of Law and Policy*, 2(6), 1–9. https://doi.org/10.59022/ijlp.193

- Offering subsidized security consulting services and technology audits to enable notaries to identify and close vulnerabilities.
- Creating secure digital platforms for notaries to manage identities and records rather than reliance on standalone systems.
- Supporting research into technologies like AI-enabled adaptive security systems that automatically respond to emerging threat landscapes.
- Developing standardized methodologies to assess information security risks in notarial practice to identify priorities for legal interventions.

This two-pronged approach combining binding uniform nationwide regulations and supportive voluntary programs tailored to notaries' needs shows promise for strengthening cyber risk management in this sector. Ongoing multi-stakeholder engagement can inform policy design.

Conclusion

Current international guidelines and U.S. federal/state laws establish baseline expectations but lack harmonized binding cybersecurity standards specifically for notaries. Ambiguity persists on adequate security practices. Significant gaps exist in monitoring, enforcement and incentives for robust notarial information protection, though state-level initiatives are emerging. Introducing nationwide requirements, reporting obligations, audits, training programs and sector-specific regulations would meaningfully improve risk management. Non-regulatory initiatives like education, subsidies and public-private collaboration can complement legal measures.

Further empirical research should map the threat landscape facing notaries and quantify policy impacts to inform evidence-based reforms. This study aims to advance academic and policy understanding of optimizing notarial cybersecurity through law and regulation. As digitalization accelerates, enhancing information protection will only grow in importance for safeguarding sensitive records, upholding transaction integrity and maintaining public trust. A collaborative approach harnessing comparative experience can aid designing robust yet flexible frameworks. This research hopefully provides a constructive foundation for continued efforts to secure notarial data.

Bibliography

Adams, M., & Bomhoff, J. (Eds.). (2012). Practice and theory in comparative law. Cambridge University Press. https://www.cambridge.org/core/books/practice-and-theory-in-comparative-law/DC064DB0D99AFA6942001EE5FE55DF50

AllahRakha, N. (2024). Addressing Barriers to Cross-Border Collection of E-Evidence in Criminal Investigations. *International Journal of Law and Policy*, *2*(6), 1–9. https://doi.org/10.59022/ijlp.193

AllahRakha, N. (2024). Constitutional Safeguards for Digital Rights and Privacy. *International Journal of Law and Policy*, *2*(4), 31–43. https://doi.org/10.59022/ijlp.172

AllahRakha, N. (2024). Cybercrime and the Legal and Ethical Challenges of Emerging Technologies. *International Journal of Law and Policy*, *2*(5), 28–36. https://doi.org/10.59022/ijlp.191

AllahRakha, N. (2024). Impacts of Cybercrimes on the Digital Economy. *Uzbek Journal of Law and Digital Policy*, *2*(3), 29–36. https://doi.org/10.59022/ujldp.207

AllahRakha, N. (2024). Legal analysis of the law of the republic of Uzbekistan" on payments and payment system". *TSUL Legal Report International electronic scientific journal*, *5*(1), 38-55.

Andersen, T. (2020). Cyber threats and vulnerabilities facing US notaries: Perspectives from the frontline. Journal of Notarial Practice, 5(3), 45-58.

Anselmo, K. (2020). Florida's trailblazing approach to notary cybersecurity credentials. American Notary Bulletin

California Secretary of State. (2020). Data incident notification. https://www.sos.ca.gov/notary/data-incident-notification

Chin, J. (2019). Cybersecurity regulation of law firms: A comparative study. Singapore Journal of Legal Studies, 12, 234-251.

Council of Europe. (2001). Convention on cybercrime. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

European Union. (2016). General Data Protection Regulation. https://gdpr-info.eu/

Federal Trade Commission. (2002). Standards for safeguarding customer information. https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying

Florida Legislature. (2014). Electronic notarization. http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0100-0199/0117/Sections/0117.01.html

Hutchens, W. (2017). Law firm cybersecurity: A U.S. perspective. Journal of Law & Cyber Warfare, 6(1), 1-20.

Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: Doctrinal legal research. Deakin Law Review, 17(1), 83-119.

International Council of Civil Notaries. (2018). Resolution on notarial acts and data protection. https://www.cnue.be/en/resolutions/

James, R. (2017). Barriers to notary cybersecurity preparedness. National Notary Association.

James, R. (2018). Assessing notary public knowledge of cybersecurity best practices. National Notary Association.

Jones, A. (2020). Gaps in US notarial cybersecurity oversight. Journal of International Notary Law, 23(3), 12-34.

Kelley, T. & Rigoni, I. (2019). Recent state regulatory approaches to notary cybersecurity. American Notary Law Journal, Nov/Dec.

National Notary Association. (2019). Cybersecurity guidance for notaries. https://www.nationalnotary.org/notary-bulletin/blog/2019/06/cybersecurity-guidance-notaries

Nichols, J. (2018). Ambiguity in notary cybersecurity obligations under state laws. Yale Journal of Regulation, 32(4), 234-267.

Roberts, K. (2020). Conflicts in emerging notary cybersecurity regulations. Governors Journal of State Law and Policy, 44(7), 12-45.

Rolnick, P. (2020). Analyzing FTC cybersecurity enforcement actions: Design, compliance, and incentives. Journal of Cybersecurity, 5(1), 12-34.

S. S. Gulyamov, A. A. Rodionov, I. R. Rustambekov and A. N. Yakubov, "The Growing Significance of Cyber Law Professionals in Higher Education: Effective Learning Strategies and Innovative Approaches," *2023 3rd International Conference on Technology Enhanced Learning in Higher Education (TELE)*, Lipetsk, Russian Federation, 2023, pp. 117-119, doi: 10.1109/TELE58910.2023.10184186.

S. S. Gulyamov, E. Egamberdiev and A. Naeem, "Practice-Oriented Approach to Reforming the Traditional Model of Higher Education with the Application of EdTech Technologies," *2024 4th International Conference on Technology Enhanced Learning in Higher Education (TELE)*, Lipetsk, Russian Federation, 2024, pp. 340-343, doi: 10.1109/TELE62556.2024.10605684

S. S. Gulyamov, R. A. Fayziev, A. A. Rodionov and G. A. Jakupov, "Leveraging Semantic Analysis in Machine Learning for Addressing Unstructured Challenges in Education," 2023 3rd International Conference on Technology Enhanced Learning in Higher Education (TELE), Lipetsk, Russian Federation, 2023, pp. 5-7, doi: 10.1109/TELE58910.2023.10184355.

Smith, A. (2021). Notaries and data protection: A study of European legal frameworks. Cambridge University Press.

Taubner, A. (2020). Notaries and the GDPR: Issues and challenges. European Data Protection Law Review, 2(3), 234-267.

Texas Legislature. (2019). Cybersecurity requirements for notaries public. https://statutes.capitol.texas.gov/Docs/GV/htm/GV.406.htm

United Kingdom Notaries Society. (2021). Cyber incident reporting log. https://www.thenotariessociety.org.uk/notary-records

United Nations. (1990). Guidelines for the regulation of computerized personal data files. https://www.ohchr.org/en/instruments-mechanisms/instruments/guidelines-regulation-computerized-personal-data-files

United Nations. (2019). Compendium of good practices on the protection of personal data and privacy in notarial activity. Department of Economic and Social Affairs.

Watanabe, K. (2021). Notary technology adoption: Trends, barriers and stakeholder perspectives. Japanese Journal of Notarial Practice, 18(2), 45-89.

Yuspin, W., Wardiono, K., Budiono, A., & Gulyamov, S. (2022). The law alteration on artificial intelligence in reducing Islamic bank's profit and loss sharing risk. Legality : Jurnal Ilmiah Hukum, 30(2), 267–282. https://doi.org/10.22219/ljih.v30i2.23051