Al-Fikru: Jurnal Ilmiah
Vol. 20 No. 2 (2026)
https://jurnal.staiserdanglubukpakam.ac.id/index.php/alfikru

P-ISSN: 1978-1326
E-ISSN: 2721-4397

PROTECTION OF USERS' CONSTITUTIONAL RIGHTS IN RELATION TO THEIR DATA IN THE DIGITAL ELECTRONIC HEALTH ALERT CARD HEALTHCARE APPLICATION: A Siyasah Dusturiyah Perspective

Ajeng Permata Zuhuriani Siregar, Khalid

Universitas Islam Negeri Sumatera Utara
Jl. William Iskandar Pasar V Medan Estate, Deli Serdang Sumatera Utara
Email: ajeng0203203125@uinsu.ac.id, khalid@uinsu.ac.id

Abstract: This study examines the protection of citizens' constitutional rights in the Electronic Health Alert Card (e-HAC) data breach case through the perspectives of Indonesian constitutional law and fiqh siyasah dusturiyah. The study focuses on the state's responsibility to safeguard sensitive health information, prevent unauthorized access, and provide remedies for affected individuals. It adopts a normative legal approach by examining relevant constitutional provisions, personal data protection legislation, and Islamic principles of governance. The analysis highlights that breaches involving government-managed health data raise concerns extending beyond technical security failures to the fulfillment of constitutional obligations. Article 28G(1) of the 1945 Constitution provides a basis for protecting personal security and dignity, while fiqh siyasah dusturiyah emphasizes amanah, justice, and public welfare in the exercise of state authority. Integrating these perspectives offers a framework for assessing governmental accountability and strengthening the ethical foundations of digital health governance. The study underscores the importance of preventive safeguards, transparent data management, and accessible remedies in protecting citizens' rights in contemporary digital governance.

Keywords: Constitutional Rights, Personal Data Protection, Siyasah Dusturiyah

Abstrak: Penelitian ini mengkaji perlindungan hak konstitusional warga negara dalam kasus kebocoran data Electronic Health Alert Card (e-HAC) melalui perspektif hukum tata negara Indonesia dan fiqh siyasah dusturiyah. Penelitian ini berfokus pada tanggung jawab negara dalam melindungi informasi kesehatan yang bersifat sensitif, mencegah akses tidak sah, serta menyediakan mekanisme pemulihan bagi individu yang terdampak. Penelitian menggunakan pendekatan hukum normatif dengan mengkaji ketentuan konstitusi, peraturan perundang-undangan tentang perlindungan data pribadi, serta prinsip-prinsip pemerintahan dalam Islam. Analisis menunjukkan bahwa kebocoran data kesehatan yang dikelola pemerintah tidak hanya berkaitan dengan kegagalan keamanan teknis, tetapi juga menyangkut pemenuhan kewajiban konstitusional negara. Pasal 28G ayat (1) UUD 1945 memberikan landasan perlindungan keamanan pribadi dan martabat manusia, sedangkan fiqh siyasah dusturiyah menekankan prinsip amanah, keadilan, dan kemaslahatan dalam penyelenggaraan kekuasaan negara. Integrasi kedua perspektif tersebut memberikan kerangka untuk menilai akuntabilitas pemerintah dan memperkuat landasan etis tata kelola kesehatan digital. Penelitian ini menegaskan pentingnya perlindungan preventif, pengelolaan data yang transparan, serta mekanisme pemulihan yang dapat diakses masyarakat dalam menjamin hak konstitusional warga negara.

Kata Kunci: Hak Konstitusional, Perlindungan Data Pribadi, Siyasah Dusturiyah

INTRODUCTION

Digital transformation in the delivery of public services is an inevitable feature of the modern state, including in the healthcare sector. The use of the Electronic Health Alert Card (e-HAC) application as a public health control instrument, particularly in relation to mobility and health emergencies, forms part of the state's policy to safeguard public safety. Nevertheless, the use of digital technology also entails serious risks, particularly concerning the protection of citizens' personal data.

Technology enables the state to manage population data more rapidly and in a more integrated manner when delivering healthcare services. Within this context, e-HAC serves as a data-based instrument for public health surveillance. When developing laws and public policy instruments in Indonesia, the government must consistently adhere to sound principles of legislative drafting and ensure accountability for protecting citizens' rights (Khalid, 2014). However, digital services that collect citizens' identity and health data must incorporate adequate data protection to prevent violations of those rights.

The Electronic Health Alert Card (e-HAC) data breach raises fundamental constitutional concerns because it involves the rights to privacy and personal security, as well as the state's responsibility to protect citizens' human rights. A data breach is not merely a technical or administrative issue; it may also reflect the state's failure to exercise due care in fulfilling its constitutional obligations. Personal data breaches can have serious consequences, including identity theft, fraud, and potential threats to national security (Al Baihaqy et al., 2025).

The collection and management of personal data by the state create risks of human rights violations unless adequate safeguards are in place (Kim, 2022). The health data processed through the Electronic Health Alert Card (e-HAC) application, which the government developed as part of its digital healthcare policy (Raposo, 2023), particularly to control mobility and monitor public health, constitute sensitive personal data. Their disclosure can lead to discrimination, privacy violations, and threats to citizens' sense of security.

The state collects and manages citizens' personal data, including sensitive identity and health information. In 2021, however, weaknesses in the e-HAC system's security were found to have resulted in a data breach, allowing unauthorized parties to access users' data. The data breaches involving PeduliLindungi and e-HAC demonstrate weaknesses in the protection of personal data managed by the state. Yet the rights to protection of one's person and to personal security are constitutional rights guaranteed by the 1945 Constitution of the Republic of Indonesia. Technically, the e-HAC breach resulted from the use of an Elasticsearch database without encryption or password protection—an unprotected server. In the absence of these basic safeguards, external parties could access the server openly without authentication. The vulnerability was first

identified by the vPnMentor cybersecurity team and reported to the National Cyber and Crypto Agency (BSSN) and the Ministry of Health before the server was eventually shut down in August 2021.

The e-HAC case was not an isolated incident in the operation of government electronic systems. Rather, it formed part of a series of similar incidents directly connected to threats to citizens' constitutional rights (Kemenkes, 2021). Other major incidents include the following: (1) the June 2024 hacking of the Temporary National Data Center (PDNS 2) operated by the Ministry of Communication and Informatics/BSSN, in which a Brain Cipher ransomware attack locked data belonging to 282 government agencies, disrupted public services, and threatened the confidentiality of citizens' data; (2) the suspected 2023 breach of 337 million population records held by the Directorate General of Population and Civil Registration at the Ministry of Home Affairs, which were offered for sale on a hacker forum and included national identification numbers, full names, and family card numbers; and (3) the 2021 breach of 279 million BPJS Kesehatan records, including participants' medical histories and personal identity information.

The Electronic Health Alert Card data breach raises fundamental constitutional concerns because it involves the rights to privacy and personal security, as well as the state's responsibility to protect citizens' human rights. A data breach is not merely a technical or administrative issue; it may also reflect the state's failure to exercise due care in fulfilling its constitutional obligations. Unfortunately, advances in information technology also create opportunities for criminal activity in cyberspace, particularly in data management. Personal data breaches can have serious consequences, including identity theft, fraud, and potential threats to national security (Al Baihaqy et al., 2025).

The collection and management of personal data by the state create risks of human rights violations unless adequate safeguards are in place (Greenleaf, 2014; Kim, 2022). The government developed the Electronic Health Alert Card (e-HAC) application as part of its digital healthcare policy (Raposo, 2023), particularly to control mobility and monitor public health. The health information processed through the application constitutes sensitive personal data, the disclosure of which can lead to discrimination, privacy violations, and threats to citizens' sense of security.

The state collects and manages citizens' personal data, including sensitive identity and health information. In 2021, however, weaknesses in server security were found to have caused a breach of the e-HAC system, enabling unauthorized parties to access users' data. The data breaches involving PeduliLindungi and e-HAC demonstrate weaknesses in the protection of personal data managed by the state. Yet the rights to protection of one's person and to personal security are constitutional rights guaranteed by the 1945 Constitution of the Republic of Indonesia.

The constitutional rights enshrined in the 1945 Constitution of the Republic of Indonesia encompass 40 citizens' rights. One is the right to protection of one's person. Article 28G(1) broadly provides that citizens are entitled to protection of their persons, families, honor, dignity, and property under their control (Sari, 2023).

In a state governed by the rule of law, protecting human rights is a constitutional obligation of the state. Article 28G(1) of the 1945 Constitution explicitly guarantees the rights to protection of one's person and to personal security (Asshiddiqie, 2011). Accordingly, the e-HAC data breach must be understood as a constitutional issue rather than solely as a technical problem.

As reported by the BBC (Andi Firdaus BBC, 2021), Indonesia experienced a breach involving the Electronic Health Alert Card (e-HAC) data of 1.3 million users, exposing PCR test results, identification numbers, and other sensitive information (Persadha, 2021). This account was further supported by a Ministry of Health report (Kemenkes, 2021) concerning a suspected breach of the old e-HAC application, which had been deactivated on July 2, 2021.

Efforts to address application data breaches should focus on restoring and strengthening individuals' control over their personal data by limiting data collection, ensuring transparent management, implementing adequate safeguards, and establishing mechanisms for accountability and remedies for data subjects (Alan, 1967).

Furthermore, data breaches should be addressed through a Privacy by Design approach, which integrates data protection into system design from the outset. This approach enables the structural prevention of breaches through security measures, protection throughout the data lifecycle, system transparency, and respect for data subjects' rights (Ann Cavoukian, 2010).

From a constitutional law perspective, the state has a constitutional obligation to respect, protect, and fulfill citizens' fundamental rights. In managing digital healthcare services, this obligation includes ensuring the security and confidentiality of the personal data that citizens entrust to the state. The e-HAC data breach raises questions about how the state discharges its responsibility to protect citizens' constitutional rights. It is therefore necessary to examine the extent to which the state has fulfilled its obligations to prevent breaches, address their consequences, and provide protection and remedies for affected citizens.

In fiqh siyasah, rulers (ulil amri) are obliged to safeguard the public interest (hifz al-maslahah), protect the people's fundamental rights, and prevent all forms of injustice and harm. Data breaches violate the principles of maqasid al-shari'ah, including hifz al-nafs (protection of life and personal security), hifz al-'ird (protection of honor and dignity), and hifz al-mal (protection of property). This position is consistent with Denny Yusmahendra's findings (Denny, 2025) on fiqh siyasah dusturiyah and personal data protection under Article 65 of Law No. 27 of 2022 on Personal Data Protection. That provision accords with Qur'an 24:27 (Surah An-Nur),

which addresses Islam's respect for and protection of an individual's private sphere. It also accords with fiqh siyasah dusturiyah, which examines state legislation directed toward the public good and the fulfillment of citizens' rights. Protecting personal data is therefore one manifestation of fulfilling every citizen's rights.

National law, through legislation and implementing regulations, provides a formal, legally binding framework for protecting health data. This framework encompasses definitions of personal data, data subjects' rights, the obligations of data controllers and processors, enforcement mechanisms, sanctions, and dispute resolution procedures. The strength of national law lies in its legitimate authority, enforceability by state institutions, and universal application to citizens regardless of religious background. Legislation such as Law No. 27 of 2022 on Personal Data Protection (the PDP Law), Law No. 11 of 2008 on Electronic Information and Transactions (the ITE Law), as amended, and health-specific regulations, including Law No. 17 of 2023 on Health and various regulations issued by the Minister of Health, has established a strong foundation. Nevertheless, national law's predominantly positivist orientation may not fully address the deeper ethical, moral, and spiritual dimensions that matter to some communities, particularly in sensitive areas such as health data.

Fiqh siyasah, by contrast, offers a rich ethical and moral perspective rooted in Islamic principles oriented toward public welfare and the prevention of harm. As a branch of Islamic jurisprudence concerned with state governance and public policy under Islamic law, fiqh siyasah provides a philosophical and ethical foundation for lawmaking and policymaking. Fundamental principles such as maslahah mursalah (public interests not specifically addressed by textual evidence but consistent with the objectives of Islamic law), maqasid al-shari'ah (the objectives of Islamic law, including the protection of religion, life, intellect, lineage, and property), justice, and the responsibility of ulil amri (leaders or rulers) to safeguard public welfare are highly relevant to health data protection. The strength of fiqh siyasah lies in its capacity to confer moral and ethical legitimacy, encourage voluntary compliance grounded in religious awareness, and guide responses to emerging issues through ijtihad.

Synergy and complementarity between national law and fiqh siyasah can develop in five areas: (1) strengthening ethical and moral foundations; (2) addressing legal gaps or ambiguities; (3) formulating more comprehensive policies; (4) enhancing public trust; and (5) establishing multiple layers of accountability.

Integrating the principles of fiqh siyasah into public policy offers a comprehensive ethical framework for governance that promotes justice, welfare, and the public good. As a branch of Islamic jurisprudence addressing state affairs, government, and public administration, fiqh siyasah provides both legal norms and moral and ethical guidance derived from

Islamic teachings. In modern public policy, this integration does not mean replacing the existing system of positive law. Rather, it enriches policy formulation, implementation, and evaluation through strong ethical, spiritual, and social dimensions, particularly in Muslim-majority countries or in policies with significant effects on Muslim communities.

From the perspective of fiqh siyasah, state power is understood as a trust that must be exercised to promote public welfare (Al-Mawardi, 2006). Every public policy, including digital policy, must prioritize the protection of the people's dignity and interests. Against this background, this article examines the protection of citizens' constitutional rights in the e-HAC data breach case through the perspectives of constitutional law and fiqh siyasah.

This study employs fiqh siyasah dusturiyah as a normative perspective for evaluating the exercise of state power and the implementation of public policies according to the principles of amanah and public welfare. Thus, fiqh siyasah dusturiyah does not replace positive law; instead, it strengthens the analysis of the state's responsibility to protect citizens' rights.

This study integrates constitutional law and fiqh siyasah dusturiyah to analyze the protection of constitutional rights and state responsibility in the e-HAC data breach case. From the constitutional law perspective, this protection rests on the rights to protection of one's person and to personal security guaranteed by Article 28G(1) of the 1945 Constitution of the Republic of Indonesia, together with provisions governing personal data protection. Meanwhile, fiqh siyasah dusturiyah evaluates state responsibility through the principles of amanah and maslahah: public affairs must be managed responsibly, with a commitment to public welfare and the prevention of harm. These perspectives therefore complement one another in assessing the extent to which the state has protected citizens' rights when managing data in e-HAC services.

The urgency of this study lies in the need to address the growing risks to citizens' constitutional rights arising from personal data breaches in government-managed digital healthcare services. The e-HAC case highlights the critical importance of evaluating the state's constitutional responsibility to ensure data security, protect individual privacy, and provide appropriate remedies for affected citizens. Furthermore, examining this issue through constitutional law and fiqh siyasah dusturiyah is essential to establishing a comprehensive understanding of state accountability that encompasses both legal obligations and ethical principles. Therefore, this study is necessary to strengthen the conceptual foundations of personal data protection and promote public policies that prioritize constitutional rights, justice, and public welfare in the digital era.

Several relevant studies help clarify this study's novelty. Makfirah (2024) examined personal data protection but focused on electoral law through the

Political Party Information System (SIPOL). Triarianto (2023) addressed the prevention of data breaches under the PDP Law in general and the educational role of the wazir tanfidz. Similarly, Putri Eka (2023) analyzed the government's general responsibility for data protection from a siyasah dusturiyah perspective, while Harahap (2023) focused on protecting the political rights of persons with disabilities. Unlike these studies, the present research focuses specifically on the e-HAC digital data breach by integrating two complementary perspectives: the protection of constitutional rights under Indonesian constitutional law and the principle of public welfare (tasarruf al-imam) in fiqh siyasah dusturiyah.

Accordingly, this study aims to analyze the protection of citizens' constitutional rights in the e-HAC data breach case, examine the state's responsibility for the breach, and assess the case from the perspective of fiqh siyasah dusturiyah.

METHOD

This study employs a normative legal research methodology, also referred to as doctrinal legal research, to examine the legal reasoning underlying the granting of marriage dispensation by the Sharia Court. Normative legal research primarily focuses on the analysis of legal norms, statutory provisions, judicial decisions, and relevant legal scholarship (Marzuki, 2021). To avoid ambiguity with empirical legal research, this study adopts a case approach, in which judicial decisions are treated as primary legal materials rather than empirical field data. This approach is complemented by a statutory approach and a conceptual approach.

The statutory approach is used to examine the relevant legal framework governing marriage dispensation and child protection, particularly Law No. 16 of 2019 amending Law No. 1 of 1974 on Marriage, Law No. 35 of 2014 on Child Protection, Supreme Court Regulation (PERMA) No. 5 of 2019 concerning Guidelines for Adjudicating Marriage Dispensation Applications, and the Compilation of Islamic Law (KHI). The conceptual approach is employed to critically assess the judicial reasoning through the perspectives of Maqāṣid al-Sharī'ah and the best interests of the child principle, thereby enabling an evaluation of whether the decision adequately reflects both Islamic legal objectives and contemporary child protection standards.

Consistent with library-based legal research (Muhaimin, 2020), the legal materials in this study are classified into three categories. Primary legal materials consist of authoritative and binding legal sources, namely the Lhokseumawe Sharia Court Decision No. 22/Pdt.P/2025/MS.LSM, Law No. 16 of 2019, Law No. 35 of 2014, PERMA No. 5 of 2019, and the Compilation of Islamic Law. Secondary legal materials include peer-reviewed journal articles, classical and contemporary fiqh literature, scholarly works on Maqāṣid al-Sharī'ah, legal commentaries, and previous studies concerning child marriage, marriage

dispensation, judicial reasoning, and child protection. Tertiary legal materials include legal dictionaries, encyclopedias, and other reference works used to clarify relevant legal concepts and terminology.

To strengthen the academic reliability of the study, secondary legal materials were systematically identified through reputable academic databases, including Scopus, Google Scholar, Sinta, and DOAJ, with priority given to peer-reviewed publications issued between 2020 and 2026. Earlier authoritative works were retained where they were considered foundational to the theoretical or jurisprudential framework. The selection of literature was based on its direct relevance to marriage dispensation, judicial reasoning, child rights, Maqāṣid al-Sharīʿah, and Islamic family law. Source credibility was further assessed by comparing scholarly arguments with statutory provisions, judicial doctrine, and recognized classical and contemporary Islamic jurisprudence.

The collected legal materials were analyzed using a descriptive-analytical and prescriptive legal analysis (Soekanto & Mamudji, 2015). The analysis was conducted through five stages of legal reasoning. First, the relevant legal facts were identified from Decision No. 22/Pdt.P/2025/MS.LSM, including the minor's age of 16 years, parental psychological concerns, and the social circumstances surrounding the application. Second, the judge's legal considerations were examined to identify the principal legal reasoning and the ratio decidendi underlying the decision. Third, vertical and horizontal norm synchronization was conducted to assess the consistency of the ruling with Law No. 16 of 2019, Law No. 35 of 2014, PERMA No. 5 of 2019, and other relevant legal norms. Fourth, the judicial reasoning was critically evaluated through the five principal dimensions of Maqāṣid al-Sharīʿah, namely ḥifẓ al-dīn, ḥifẓ al-nafs, ḥifẓ al-ʿaql, ḥifẓ al-nasl, and ḥifẓ al-māl, and was simultaneously assessed against the best interests of the child principle. Fifth, a critical legal synthesis was formulated to determine whether the decision substantially promotes long-term child protection or primarily accommodates parental moral and psychological concerns.

The interpretive process also considered possible conflicts among statutory norms, Islamic legal doctrines, and judicial considerations. Statutory conflicts were addressed through established principles of legal interpretation, particularly lex superior derogat legi inferiori and lex specialis derogat legi generali. Where tension arose between classical fiqh opinions and contemporary positive law, the analysis applied tarjīḥ, understood as contextual legal weighting, together with the principles of siyāsah sharʿiyyah and Maqāṣid al-Sharīʿah. These interpretive principles were used to prioritize legal reasoning that provides stronger protection for the child's long-term physical, psychological, educational, social, and developmental interests over short-term considerations of moral anxiety.

RESULTS AND DISCUSSION

Protection of Citizens' Constitutional Rights in the e-HAC Data Breach Case

The protection of Electronic Health Alert Card (e-HAC) users' data must be situated within the relationship between the state's authority to provide healthcare services and its obligation to protect constitutional rights. Health applications enable the government to collect information for disease control and mobility monitoring. These objectives, however, do not confer unlimited authority to collect, retain, or share citizens' data. This study's normative analysis treats users as rights holders whose interests must be considered throughout data processing. Accordingly, successful digitalization should be measured not only by service speed or user numbers but also by service providers' ability to ensure confidentiality, appropriate use, and accountability for the information they manage.

The constitutional basis for this protection lies in Article 28G(1) of the 1945 Constitution of the Republic of Indonesia, which concerns the protection of one's person, honor, dignity, and personal security. This provision relates to Article 28H(1) on the right to healthcare and Article 28I(4) on the state's responsibility to protect human rights. A systematic reading indicates that healthcare provision and privacy protection are obligations that must be fulfilled concurrently. The state should not force citizens to choose between accessing necessary services and relinquishing all control over their personal information. This relationship provides a basis for evaluating whether service design adequately limits the exercise of authority.

Citizens' constitutional rights are fundamental rights guaranteed explicitly or implicitly by the constitution and binding on all actions of state institutions. These rights serve a dual function: they protect citizens while limiting state power to ensure that the government remains subject to the rule of law (rechtsstaat) (Muhtar et al., 2023). Within the framework of the 1945 Constitution of the Republic of Indonesia, Chapter XA comprehensively addresses these rights. Article 28G(1) specifically guarantees protection of one's person, family, honor, and dignity, as well as the right to personal security (Willa Wahyuni, 2023).

As public services become digitalized, personal data protection becomes a crucial dimension of fulfilling these constitutional rights. The Electronic Health Alert Card (e-HAC) was a government healthcare instrument used during the COVID-19 pandemic that required citizens to submit sensitive personal data, including identity information and medical records. Unfortunately, in 2021, the old e-HAC system experienced a breach because it used an Elasticsearch database without encryption or password protection—an unprotected server. Consequently, the data of approximately 1.3 million users were exposed, including identification

numbers, PCR test results, and other sensitive information (Andi Firdaus BBC, 2021).

Viewed in light of Article 28G(1) of the 1945 Constitution of the Republic of Indonesia, the e-HAC data breach cannot be reduced to a technical or administrative problem or a cybersecurity failure alone. Personal data represent citizens' private sphere. The state's failure to protect these data directly threatens citizens' personal security and dignity and may facilitate identity theft and fraud.

Although the e-HAC incident preceded the enactment of Law No. 27 of 2022 on Personal Data Protection (the PDP Law), Government Regulation No. 71 of 2019 on the Operation of Electronic Systems and Transactions had already established data protection obligations. Government electronic systems must operate reliably, securely, and accountably. Data protection in e-HAC services is therefore a pressing constitutional concern because it directly relates to the state's positive obligation to safeguard its citizens' fundamental rights.

Nevertheless, an assessment of the e-HAC case must begin with an accurate account of its factual status. On August 31, 2021, the Ministry of Health reported a suspected breach involving the old e-HAC application and stated that further investigation was necessary. On September 9, 2021, the ministry explained that the police investigation had found no evidence of data being taken from the e-HAC server (Kemenkes, 2021). These statements must be presented together. This article cannot conclude that all initial reports were substantiated, nor can it treat the absence of evidence of data extraction as proof that every aspect of governance met the required standards. These two issues require different objects of inquiry and types of evidence.

This distinction yields three levels of analysis. The first concerns vulnerabilities: conditions that permit unauthorized access. The second concerns incidents: demonstrable events involving access, disclosure, alteration, or loss of data. The third concerns consequences: losses or infringements of users' rights. A vulnerability requires preventive action even when no resulting harm has been established. By contrast, particular claims for accountability require additional evidence concerning the obligation breached, the responsible party, and the connection to the consequences. This framework prevents constitutional analysis from becoming an accusation that exceeds the evidence, while ensuring that the government does not disregard risks merely because harm has not yet been quantified.

A further issue concerns the imbalance between providers and users. Citizens generally cannot examine system configurations, technology vendor contracts, or the identities of those accessing their data. Our Data, Ourselves addresses everyday privacy concerns, including health data and government use of information (Lipton, 2022). In this study, that discussion helps situate privacy within the exercise of power over

information. However, greater user awareness must not replace institutional responsibility. Advising citizens to exercise caution when sharing data offers limited protection when providing those data is a condition of service and no comparable alternative is available.

The authority to collect data must therefore be assessed against the principles of necessity and proportionality. Providers must explain the connection between each category of data and the intended health objective. Information that is generally useful is not necessarily required for a particular purpose. Combining identity information, test results, and travel records, for example, requires an assessment of both operational benefits and re-identification risks. This study proposes that such an assessment address clarity of purpose, the availability of less privacy-intrusive alternatives, retention limits, and oversight mechanisms. This test is a normative analytical tool; a finding that e-HAC failed to satisfy it would still require relevant design documents, processing policies, and investigative findings.

International comparisons clarify the importance of these limitations. Raposo (2023) explains that pandemic-response technologies support public health control while creating risks to privacy and liberty, necessitating governance and restrictions. In the South Korean context, Kim (2022) examines uncertainty over the balance between privacy protection and effective disease control. The present study aligns with both accounts in rejecting the assumption that emergencies eliminate the need for oversight. Its distinctive focus is on the obligations of Indonesian public service providers. Other countries' experiences serve as conceptual comparisons rather than grounds for assuming that their legal structures and institutional capacities are identical.

The temporal dimension also determines the accuracy of legal arguments. Reports concerning e-HAC emerged in 2021, whereas Law No. 27 of 2022 on Personal Data Protection was not promulgated until October 17, 2022. At the time of the reported incident, Government Regulation No. 71 of 2019 already contained principles governing personal data protection. The absence of the PDP Law in 2021 therefore did not mean that no protection obligations existed. Nevertheless, the article must distinguish an assessment under the rules applicable at the time from the use of the PDP Law as a subsequent development in regulatory standards. This distinction safeguards legal certainty and prevents the retrospective imposition of obligations or sanctions without an appropriate basis (Komunikasi & Indonesia, 2022).

In Indonesia, Makfirah (2024) links data protection in SIPOL to constitutional rights and emphasizes oversight, verification, and complaint resolution. The e-HAC study supports the importance of these mechanisms but extends the discussion to health information, which may produce different

social consequences. Misuse of identity information in political administration and disclosure of health conditions both undermine individuals' control over information, but they do not necessarily require identical remedies. Protection policies must therefore consider the context of data use, the relationship between users and providers, and potential consequences for everyday life. Shared principles do not eliminate differences in operational needs.

Constitutional protection also encompasses users' ability to obtain explanations and raise objections. A privacy policy that is available but difficult to understand does not necessarily provide meaningful transparency. Providers should explain processing purposes, the parties involved, retention limits, and complaint channels in accessible language. The state must also consider users with limited digital literacy so that protection procedures do not benefit only those who understand technical terminology. Equality in this context requires usable procedures rather than merely the formal recognition of rights. Indicators of success may include the accessibility of complaint services and the clarity of follow-up on users' requests. The contribution of constitutional analysis in the e-HAC case thus lies in shifting the evaluative focus from the existence of an application to the quality of the constraints on power over data. The government must be able to demonstrate its reasons for processing data, the safeguards implemented, and accountable review mechanisms. Findings concerning specific violations remain dependent on evidence, whereas preventive duties need not await actual harm. The theoretical implication is that digital healthcare services provide a setting both for realizing rights and for potentially restricting them. In practice, system evaluation must connect technical security to users' needs, institutional openness, and access to effective remedies.

A Siyasah Dusturiyah Analysis of the e-HAC Data Breach Case

Fiqh siyasah dusturiyah is a branch of fiqh siyasah concerned with the principles governing the exercise of power, relations between the government and the people, and the fulfillment and protection of public rights. In the context of personal data protection, this perspective assesses the government's responsibility to safeguard citizens' data according to the principle of preventing harm. Personal data submitted to the government through digital public services constitute a trust that must be managed responsibly and must not cause harm to the public.

The state's duty to uphold this public trust is explicitly affirmed in Qur'an 4:58 (Surah An-Nisa) (Depag RI, 1998), which commands that trusts be returned to those entitled to them and that the authorities judge justly. Imam al-Mawardi reinforces this command in his seminal work al-Ahkam al-Sultaniyyah, stating:

وَالإِمَامَةُ مَوْضُوعَةٌ لِخِلَافَةِ النُّبُوَّةِ فِي حِرَاسَةِ الدِّينِ وَسِيَاسَةِ الدُّنْيَا

"The imamate is established to succeed prophethood in safeguarding religion and governing worldly affairs."

This theoretical statement indicates that rulers have an absolute obligation to protect the people's interests, safety, and security in all aspects of life, including the management of digital healthcare services containing citizens' sensitive data.

Furthermore, the urgency of personal data protection in Islam can be analyzed through maqasid al-shari'ah, which seeks to promote public welfare and prevent harm. The e-HAC data breach, which exposed the personal information and medical records of millions of users, potentially threatens three essential elements of public welfare within the daruriyyat al-khams:

1) Hifz al-Nafs (Protection of Life and Personal Security): The exposure of personal data can undermine data subjects' psychological well-being and sense of security.
2) Hifz al-'Ird (Protection of Honor and Dignity): The disclosure of private health information risks damaging personal honor and creating opportunities for social stigma or discrimination.
3) Hifz al-Mal (Protection of Property): The potential misuse of identity data for financial crime, fraud, or identity theft directly threatens the security of citizens' property.

Within Islamic privacy ethics, the protection of personal information also relates to the prohibition of tajassus—seeking out others' faults or spying on their private affairs—as stated in Qur'an 49:12 (QS. Al-Hujurat) (Depag RI, 1998):

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ ٱجۡتَنِبُواْ كَثِيرٗا مِّنَ ٱلظَّنِّ إِنَّ بَعۡضَ ٱلظَّنِّ إِثۡمٞۖ وَ لَا تَجَسَّسُواْ وَلَا يَغۡتَب بَّعۡضُكُم بَعۡضًاۚ أَيُحِبُّ أَحَدُكُمۡ أَن يَأۡكُلَ لَحۡمَ أَخِيهِ مَيۡتٗا فَكَرِهۡتُمُوهُۚ وَٱتَّقُواْ ٱللَّهَۚ إِنَّ ٱللَّهَ تَوَّابٞ رَّحِيمٞ ١٢

"O you who believe, avoid much suspicion, for some suspicion is indeed sinful. Do not seek out others' faults or backbite one another. Would any of you like to eat the flesh of his dead brother? Surely you would find it repugnant. And be mindful of Allah. Indeed, Allah is Ever-Accepting of repentance, Most Merciful."

Although government data collection for public health management during the pandemic is, in principle, justified, negligence in safeguarding data security systems that results in disclosure and unauthorized access constitutes a disregard for the public's right to privacy.

From a normative and philosophical standpoint, the analysis of the e-HAC incident rests on two major maxims of fiqh siyasah. The first, الضَّرَرُ يُزَالُ (ad-dararu yuzal), requires the removal and prevention of all forms of harm or loss affecting the public. The second, تَصَرُّفُ الإِمَامِ

عَلَى الرَّعِيَّةِ مَنُوطٌ بِالْمَصْلَحَةِ (tasarruf al-imam ‘ala al-ra‘iyyah manutun bi al-maslahah), means that all policies and actions of rulers concerning their people must consistently promote public welfare.

The Ministry of Health’s deactivation of the old e-HAC application on July 2, 2021, was a legitimate operational response. From the perspective of fiqh siyasah dusturiyah, however, the ruler’s responsibility cannot be limited to reactive measures after harm occurs. The principle of public welfare requires proactive safeguards and systemic prevention from the outset of data management, because failure to preserve the confidentiality of citizens’ data creates opportunities for injustice and harm to the very people who should be protected.

Siyasah dusturiyah provides a perspective for evaluating the relationship between power, the public interest, and the protection of public rights in e-HAC management. It does not seek to replace positive law but to clarify ethical accountability and the purposes for which authority is exercised. Nasrullah (2023) situates fiqh siyasah within discussions of leadership, political authority, government, justice, and their relationship to maqasid. Drawing on that scope, this study asks how the government exercises authority over citizens’ information and how that authority is constrained. Its application to digital data represents this study’s contextual reasoning rather than a claim that classical Islamic political literature directly addressed modern health technologies.

Amanah provides the starting point because the state receives information concerning people’s private lives. In this relationship, submitting data cannot be interpreted as granting unlimited authority to use them. Amanah requires management consistent with the purpose that justified receiving the information. Analytically, this study translates amanah into obligations to determine who may access data, what actions are permitted, and who verifies compliance. This translation is necessary to prevent amanah from remaining merely a judgment about individual officials’ piety. In digital systems, harm can arise from unclear responsibilities, weak procedures, or discontinuous oversight even in the absence of an intention to cause harm.

An institutional understanding of amanah also avoids the simplistic assumption that every incident constitutes intentional betrayal. Assessment must distinguish among abuse of authority, demonstrable negligence, operational error, and attacks that occur despite reasonable safeguards. This distinction does not diminish government responsibility; rather, it helps identify proportionate corrective measures. Intentional misuse requires law enforcement, while organizational weaknesses require improvements in procedures and capacity. In the e-HAC case, moral judgment preceding factual

examination could undermine the very justice being pursued. Amanah therefore entails both the obligation to protect citizens and the duty to explain events truthfully.

The principle of public welfare extends the analysis beyond administrators' conduct to the consequences of policy. The use of e-HAC can be understood as an effort to secure public health benefits, but those benefits must be weighed against the risks associated with information management. This study employs the maxim tasarruf al-imam 'ala al-ra'iyyah manutun bi al-maslahah as a normative standard requiring rulers' policies to serve the people's interests. Its application requires reasons that can be scrutinized rather than a mere invocation of the public interest. The government must demonstrate that the data collected are relevant, collection is not excessive, and safeguards are proportionate to the risks. Public welfare thus requires both evidence of benefit and control over consequences.

Public welfare also cannot be measured solely by the number of beneficiaries. A policy that benefits many people must still account for groups exposed to greater risks. Information about particular health conditions, for example, may generate stigma or unequal treatment if disclosed. A siyasah dusturiyah analysis must assess this distribution of benefits and burdens so that majority interests do not automatically justify neglecting individuals. In this study, justice requires providers to identify vulnerable users and offer protection suited to their needs. Such an assessment deepens the inquiry from whether an application is beneficial to who receives its benefits and who bears its risks.

Putri Eka (2023) directly connects government responsibility, data protection, and personal honor from a siyasah dusturiyah perspective. That study also treats irresponsible processing, not only breaches, as a protection concern. The e-HAC study shares this orientation but extends the analysis across all stages of healthcare service management. Consequently, a system still requires evaluation if it collects excessive information or retains data without an adequate purpose, even when external parties have not extracted data. This convergence demonstrates that siyasah dusturiyah can address policy design and administrative practice rather than only responses following incident reports.

The maqasid approach further helps identify the interests requiring protection. The protection of life is relevant when information supports safe healthcare; the protection of property is relevant when identity information is at risk of being used for fraud; and the protection of honor concerns possible stigma and the disclosure of private information. Nevertheless, the study must maintain classificatory precision by avoiding the automatic inclusion of hifz al-'ird among the five classical essentials without explaining its sources and

theoretical construction. For this article, honor can be discussed as a normative interest related to users' dignity. This connection is argumentative and does not itself establish that every risk has materialized as actual harm to e-HAC users.

The prevention-of-harm principle then requires policies before, during, and after processing. Before collection, providers should assess data needs and potential consequences. During service operation, administrators should monitor access and system changes. Once the collection purpose has ended, continued retention requires a defensible justification. In this study's framework, closing an application does not discharge responsibility for previously collected data. Copies, archives, and third-party access still require evaluation. This reasoning clarifies that preventing harm is a continuing obligation that follows the data rather than one that applies only while an application appears active to the public.

Research by Pandu Wijaksana et al. (2026) supports the connection between norms and implementing capacity. Their empirical study in Bandung Kidul District identified management procedures, information provision, and mitigation measures, while also finding limitations in infrastructure, budgets, and human resources. These findings do not establish identical conditions in e-HAC, but they indicate that normative commitments require organizational support. This study therefore infers that amanah must be translated into resource allocation, clear divisions of authority, and competence assessment. The government cannot merely impose security obligations without ensuring that implementing units have the capacity to fulfill them.

Siyasah dusturiyah also provides grounds for strengthening oversight and participation. As the parties supplying information, citizens need opportunities to question data use and raise objections. In the contemporary application proposed here, deliberation can support policy consultation, while accountability can be implemented through independent review and the publication of evaluation summaries. Openness must nevertheless be constrained to avoid revealing users' identities or details that increase security risks. Transparency therefore means providing relevant explanations to those entitled to receive them rather than disclosing all information without limits. Its principal measure is whether the public can evaluate government action without creating additional harm.

State Responsibility for the e-HAC Data Breach

State responsibility for the Electronic Health Alert Card (e-HAC) case derives from the principle of the rule of law (rechtsstaat), which obliges the government to provide public services while protecting citizens' constitutional rights. Digital healthcare services involving sensitive personal

information require adequate safeguards to ensure confidentiality, integrity, and security. Accordingly, state responsibility encompasses three interconnected dimensions: prevention, response, and recovery. These dimensions represent continuing constitutional obligations, although legal accountability for specific violations must be established through applicable legal provisions and supporting evidence.

A distinction must be maintained between constitutional responsibility and liability for particular incidents. Constitutional obligations require the government to establish secure information systems, implement institutional oversight, and respond appropriately to identified risks. Conversely, determining legal liability requires examining the applicable regulations, identifying responsible parties, and establishing connections between their actions and alleged violations. Therefore, reported security vulnerabilities do not automatically establish negligence or justify sanctions. Nevertheless, the absence of proven violations does not eliminate governmental obligations to strengthen preventive protection and institutional accountability.

Responsibility also involves relationships among government institutions, application developers, infrastructure providers, and other service partners. Determining accountability requires identifying who controls processing purposes, manages information, authorizes access, and supervises system operations. Law No. 27 of 2022 on Personal Data Protection distinguishes between data controllers and processors and establishes specific accountability obligations (Komunikasi & Indonesia, 2022). Although these classifications provide a useful analytical framework, they cannot automatically determine liability for incidents occurring in 2021. Such assessments must rely on the legal provisions applicable at that time and verifiable institutional relationships.

The preventive dimension requires integrating technical safeguards with effective administrative governance. Government institutions should establish legitimate purposes for collecting information, classify sensitive data, restrict unnecessary processing, and implement appropriate access controls. Preventive measures include authentication, authorization management, activity monitoring, security testing, and periodic evaluation. However, technological safeguards alone cannot guarantee protection, particularly when organizational weaknesses or inappropriate internal access remain unresolved. Effective prevention therefore depends on coordination between technological systems, institutional procedures, and professional supervision.

Preventive responsibility additionally extends to procurement arrangements and third-party oversight. Agreements with technology providers should establish responsibilities concerning information processing, access restrictions, incident reporting, confidentiality, and data management following contractual

termination. Government institutions must evaluate compliance through periodic assessments and documented supervision. Nevertheless, outsourcing does not automatically transfer all responsibility to external providers, nor does it establish governmental liability for every independent action undertaken by contractors. Accountability must instead consider actual authority, contractual obligations, operational control, and the effectiveness of institutional oversight.

The response dimension concerns governmental actions following reported vulnerabilities or suspected security incidents. Responsible institutions should promptly verify reports, preserve relevant evidence, identify potentially affected systems, and implement measures to contain risks. Investigations must distinguish technical vulnerabilities from verified unauthorized access and demonstrated information extraction. This distinction is particularly important in the e-HAC case, where public statements concerning system vulnerabilities and possible data extraction differed. Therefore, governmental accountability should be assessed through documented response procedures, investigation records, and communication transparency rather than assumptions concerning the occurrence or consequences of a breach.

Subsequent regulatory developments provide additional standards for evaluating digital governance. Article 46 of Law No. 27 of 2022 requires written notification to affected data subjects and relevant authorities within 3 × 24 hours following a personal data protection failure. Article 47 further establishes accountability obligations for data controllers (Komunikasi & Indonesia, 2022). These provisions demonstrate the importance of timely notification and demonstrable compliance. However, because the e-HAC incident occurred in 2021, these subsequent requirements cannot automatically establish violations of statutory deadlines at that time. Their relevance lies primarily in strengthening future governance and institutional preparedness.

The recovery dimension addresses the consequences experienced by affected individuals and the restoration of their rights. Technical improvements or system restoration may not adequately resolve privacy concerns, identity misuse, or other potential losses. Consequently, government institutions should provide accessible complaint mechanisms, information correction procedures, and appropriate avenues for legal remedies. Article 12 of the Personal Data Protection Law recognizes rights to pursue claims and compensation for unlawful processing under applicable legislation (Komunikasi & Indonesia, 2022). Nevertheless, compensation cannot be presumed for every e-HAC user without establishing the relevant legal basis, violation, resulting losses, and evidentiary requirements.

Effective remedies also require addressing inequalities in access to evidence. Individual users generally lack access to internal security records,

administrative communications, and technical investigation reports necessary to substantiate claims. Accordingly, authorized supervisory or judicial institutions should have appropriate mechanisms for obtaining relevant documentation while maintaining confidentiality. Such procedures can improve procedural fairness without eliminating evidentiary standards. Information disclosed during investigations must remain subject to safeguards to prevent additional exposure of sensitive personal data.

Previous studies reinforce the importance of institutional capacity and effective oversight. Makfirah (2024) emphasizes supervision and complaint mechanisms in personal data protection within the Political Party Information System (SIPOL). Similarly, Pandu Wijaksana et al. (2026) identify limitations involving organizational capacity and implementation in local digital public services. Although these findings cannot directly establish institutional failures within e-HAC, they indicate that regulatory provisions require operational resources, competent personnel, and functioning accountability mechanisms. Further investigation should therefore examine institutional contracts, audit documentation, administrative procedures, and relevant official reports.

Finally, governmental responsibility continues throughout the information lifecycle, including after an application has been discontinued. Deactivation does not automatically resolve obligations concerning stored records, archived information, remaining access permissions, or data transfers. From a siyasah dusturiyah perspective, these continuing obligations reflect amanah, requiring responsible stewardship of information entrusted by citizens. Constitutional law similarly demands that governmental authority remain subject to legal limitations and accountability. Consequently, prevention, response, and recovery should operate as an integrated governance framework, ensuring continuous protection while maintaining evidence-based determinations of specific legal liability.

CONSLUSION

This study concludes that the Electronic Health Alert Card (e-HAC) case raises significant concerns regarding the protection of citizens' constitutional rights, particularly privacy, dignity, and personal security. Article 28G(1) of the 1945 Constitution provides a constitutional foundation for protecting personal information, including sensitive health data. Consequently, digital healthcare governance must address not only technical security vulnerabilities but also the state's responsibility to safeguard fundamental rights. From the perspective of fiqh siyasah dusturiyah, personal data management represents a public trust requiring the implementation of amanah, maslahah, and mas'uliyyah. These principles emphasize governmental accountability, public welfare, and the

prevention of harm. Data protection also corresponds to maqasid al-shari'ah, particularly hifz al-nafs, hifz al-'ird, and hifz al-mal, which concern personal security, dignity, and property protection. State responsibility encompasses three interconnected dimensions: prevention, response, and recovery. Prevention requires effective security systems and institutional oversight; response demands timely investigation and transparent communication; while recovery involves corrective measures and accessible remedies for affected individuals. However, determining specific legal liability requires sufficient evidence and consideration of applicable legislation. Ultimately, integrating constitutional safeguards with Islamic governance principles strengthens accountable, rights-based digital healthcare governance and promotes sustainable public trust in government-managed information systems.

REFERENCES

Al Baihaqy, A. H., Yuwana, M. A. S. A., Surya, A. P. A., & Fauzi, M. A. N. (2025). Analisa dampak kebocoran data Pusat Data Nasional (PDN) 2024 dalam perspektif HAM. Wicarana, 4(1), 31–37. https://doi.org/-10.57123/wicarana.v3i1.167

Asshiddiqie, J. (2011). Gagasan negara hukum Indonesia [Makalah]. Forum Dialog Perencanaan Pembangunan Hukum Nasional, Badan Pembinaan Hukum Nasional, Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia.

BBC News Indonesia. (2021, August 31). Data eHAC milik 1,3 juta penggunanya dilaporkan bocor, "keamanan data tidak prioritas". https://www.bbc.com/indonesia/indonesia-58393345

Cavoukian, A., Taylor, S., & Abrams, M. E. (2010). Privacy by design: Essential for organizational accountability and strong business practices. Identity in the Information Society, 3, 405–413. https://doi.org/-10.1007/s12394-010-0053-z

Harahap, N., & Irwansyah, I. (2023). Perlindungan dan jaminan bagi penyandang disabilitas berdasarkan UU No. 7 Tahun 2017 tentang Pemilu terhadap hilangnya hak politik pada kontestasi pemilu perspektif fiqh siyasah. Al-Mashlahah: Jurnal Hukum Islam dan Pranata Sosial, 11(1), 1–14. https://doi.org/-10.30868/am.v11i01.3984

Indonesia. (2022). Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Nomor 6820. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Kementerian Agama Republik Indonesia. (1998). Al-Qur'an dan terjemahnya. Mujamma' al-Malik Fahd li Thiba'at al-Mushaf al-Sharif.

Kementerian Kesehatan Republik Indonesia. (2021, August 31). Aplikasi PeduliLindungi aman, dugaan kebocoran data pada aplikasi e-HAC yang lama. https://www.kemkes.go.id/id/aplikasi-pedulilindungi-aman-dugaan-kebocoran-data-pada-aplikasi-e-hac-yang-lama

Khalid. (2014). Ilmu perundang-undangan. Manhaji dan Fakultas Syariah IAIN Sumatera Utara.

Khallaf, A. W. (1978). 'Ilm usul al-fiqh. Dar al-Qalam.

Kim, Y. (2022). Uncertain future of privacy protection under the Korean public health emergency preparedness governance amid the COVID-19 pandemic. Cogent Social Sciences, 8(1), Article 2006393. https://doi.org/10.1080/23311886.2021.2006393

Kliwantoro, D. D. (2021, September 1). Pakar nilai respons Kemenkes lambat terkait laporan kebocoran data. ANTARA News. https://www.antaranews.com/berita/2365010/pakar-nilai-respons-kemenkes-lambat-terkait-laporan-kebocoran-data

Lipton, J. D. (2022). Our data, ourselves: A personal guide to digital privacy. University of California Press. https://www.ucpress.edu/books/our-data-ourselves/epub-pdf

Makfirah, R., Nasution, F. A., Nasution, A. H., & Afnila, A. (2024). Perlindungan data pribadi sebagai bagian dari hak konstitusional warga negara dalam Sistem Informasi Partai Politik (SIPOL). Jurnal Ilmu Hukum, Humaniora dan Politik, 4(5), 1655–1665. https://doi.org/10.38035/jihhp.v4i5.2392

Marzuki, M. (2017). Penelitian hukum (Edisi revisi). Prenada Media.

Muhtar, M. H., Maranjaya, A. K., Arfiani, N., & Rahim, E. (2023). Teori & hukum konstitusi: Dasar pengetahuan dan pemahaman serta wawasan pemberlakuan hukum konstitusi di Indonesia. PT Sonpedia Publishing Indonesia.

Nasrullah, A. M. A. (2023). Maqashid syariah: Konsep, sejarah, dan metode. Literasi Nusantara Abadi.

Raposo, V. L. (2023). Health, privacy and liberty: A call for digital governance during (and after) the pandemic. The International Journal of Human Rights, 27(3), 529–551. https://doi.org/10.1080/13642987.2022.2132234

Sari, A. K. (2023). Aspek hukum perlindungan data pribadi sebagai hak privasi pengguna media sosial. Jurnal Rectum: Tinjauan Yuridis Penanganan Tindak Pidana, 5(1), 970–980. https://doi.org/-10.46930/jurnalrectum.v5i1.2856

Soekanto, S., & Mamudji, S. (2010). Penelitian hukum normatif: Suatu tinjauan singkat. Rajawali Pers.

Triarianto, S. Y. (2023). Tinjauan siyasah dusturiyah terhadap pencegahan kasus kebocoran data pribadi masyarakat menurut Undang-Undang Perlindungan Data Pribadi No. 27 Tahun 2022 [Skripsi sarjana, Universitas Islam Negeri Sunan Ampel Surabaya]. Digilib UIN Sunan Ampel. https://digilib.uinsa-.ac.id/id/eprint/63176/

Wahyuni, W. (2023, March 9). Hak konstitusional warga negara. Hukumonline. https://www.-hukumonline.com/berita/a/hak-konstitusional-warga-negara-lt640908f758dd9/

Westin, A. F. (1967). Privacy and freedom. Atheneum.

Wijaksana, D. P., Sutiana, Y., & Alamsyah, T. (2026). The siyasah dusturiyyah perspective on personal data protection in digital public services in Bandung Kidul District, Bandung City, under Law Number 27 of 2022. Journal of Indonesian Islamic

Studies, 5(2), 762–771. https://doi.org/10.24256/jiis.v5i2.11701

Wiraguna, S. (2024). Metode normatif dan empiris dalam penelitian hukum: Studi eksploratif di Indonesia. Public Sphere: Jurnal Sosial Politik, Pemerintahan dan Hukum, 3(3). https://doi.org/10.59818/jps.v3i3.1390

Yusmahendra, D. (2025). Tinjauan fiqh siyāsah dustūriyyah terhadap Pasal 65 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi [Skripsi sarjana, Universitas Islam Negeri Raden Intan Lampung]. https://repository-.radenintan.ac.id/37646/