Indonesian Health Justice Review
ISSN: XXXX-XXXXX (Online)
Vol. 3, No. 1, 2026, pp. 27-52
Published online since March 25, 2026

Electronic Medical Record Breaches and Hospital Liability: Protecting Patients' Privacy under Indonesian Health and Data Protection Law

Siska Ayudevi*
Universitas Negeri Surabaya, Surabaya, Indonesia
siska.ayudevi@students.unesa.ac.id

DOI: https://doi.org/10.65815/hvzwtk22

Submitted: 30-08-2025	Revised: 29-11-2025, 27-02-2026	Accepted: 10-03-2026

*Corresponding Author

Abstract

The digitalization of healthcare has transformed the management and exchange of patient information through electronic medical records (EMRs). While EMRs enhance continuity and efficiency of care, they also expose highly sensitive health information to cybersecurity threats and unauthorized disclosure. This article examines the legal responsibility of hospitals when electronic medical records are leaked, accessed without authorization, or otherwise compromised. The study employs normative legal research by examining Indonesian health legislation, personal data protection regulations, and principles governing the confidentiality of medical information. Particular attention is given to the relationship between hospitals' obligations as healthcare providers and their responsibilities as entities processing sensitive personal data. The analysis finds that the existing regulatory framework establishes multiple obligations concerning confidentiality, data security, and patient rights, but the distribution of responsibility between hospitals, healthcare professionals, technology providers, and other data processors remains insufficiently articulated. This fragmented framework may create uncertainty regarding remedies and accountability following a data breach. The article argues that hospital liability should be assessed through a risk-based framework emphasizing preventive security measures, organizational control, breach notification, and effective remedies for affected patients. Strengthening institutional accountability is essential to ensure that digital healthcare development remains consistent with the fundamental right to privacy and the broader principle of health justice.

[*Digitalisasi layanan kesehatan telah mengubah pengelolaan dan pertukaran informasi pasien melalui rekam medis elektronik (EMR). Meskipun EMR meningkatkan kontinuitas dan efisiensi perawatan, EMR juga mengekspos informasi kesehatan yang sangat sensitif terhadap ancaman keamanan siber dan pengungkapan tanpa izin. Artikel ini mengkaji tanggung jawab hukum rumah sakit ketika rekam medis elektronik bocor, diakses tanpa izin, atau*

dikompromikan dengan cara lain. Studi ini menggunakan penelitian hukum normatif dengan mengkaji undang-undang kesehatan Indonesia, peraturan perlindungan data pribadi, dan prinsip-prinsip yang mengatur kerahasiaan informasi medis. Perhatian khusus diberikan pada hubungan antara kewajiban rumah sakit sebagai penyedia layanan kesehatan dan tanggung jawab mereka sebagai entitas yang memproses data pribadi yang sensitif. Analisis menemukan bahwa kerangka peraturan yang ada menetapkan berbagai kewajiban terkait kerahasiaan, keamanan data, dan hak pasien, tetapi distribusi tanggung jawab antara rumah sakit, profesional kesehatan, penyedia teknologi, dan pengolah data lainnya masih belum cukup terartikulasi. Kerangka kerja yang terfragmentasi ini dapat menciptakan ketidakpastian mengenai upaya hukum dan akuntabilitas setelah pelanggaran data. Artikel ini berpendapat bahwa tanggung jawab rumah sakit harus dinilai melalui kerangka kerja berbasis risiko yang menekankan langkah-langkah keamanan preventif, kontrol organisasi, pemberitahuan pelanggaran, dan upaya hukum yang efektif bagi pasien yang terkena dampak. Memperkuat akuntabilitas kelembagaan sangat penting untuk memastikan bahwa pengembangan layanan kesehatan digital tetap konsisten dengan hak mendasar atas privasi dan prinsip keadilan kesehatan yang lebih luas.]

Keywords: Electronic medical records, data breach, hospital liability, patient privacy, data protection

Introduction

The digital transformation of healthcare has fundamentally changed the legal character of medical information. Traditionally, patient records were maintained predominantly in physical form and were accessed within relatively bounded institutional environments. Electronic medical records (EMRs), by contrast, permit information to be stored centrally, accessed simultaneously by multiple authorized users, transferred between healthcare facilities, integrated with diagnostic systems, and processed through interconnected digital infrastructures. These characteristics generate significant benefits for continuity and efficiency of care, but they also expand the number of points at which sensitive information can be compromised. Research on electronic health records consistently identifies privacy, confidentiality, cybersecurity, interoperability, and access control as continuing challenges accompanying digitalization (Abouelmehdi, Beni-Hessane, and Khaloufi 2018; Al-Issa, Ottom, and Tamrawi 2019). The legal significance of this transformation is substantial because health information is not merely ordinary personal information. It can reveal a person's physical and mental condition, diagnosis, treatment, genetic characteristics, reproductive history, and other intimate circumstances. A breach can therefore produce consequences extending

beyond financial loss to discrimination, stigma, reputational injury, psychological distress, and violations of personal autonomy.

The Indonesian legal system has responded to healthcare digitalization through several overlapping regulatory instruments. Law Number 17 of 2023 concerning Health provides a contemporary statutory framework for health services and specifically recognizes the patient's rights to health information and access to information contained in medical records. It also requires healthcare facilities to maintain the security, integrity, confidentiality, and availability of medical-record data. Minister of Health Regulation Number 24 of 2022 concerning Medical Records complements this framework by requiring healthcare facilities to operate electronic medical records and emphasizing the principles of security and confidentiality in their management.

At the same time, Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) establishes a general data-protection framework applicable to personal-data processing, including health data. Article 4 expressly classifies health and health-information data as specific personal data, while Articles 35–47 establish obligations relating to security, confidentiality, accountability, and breach notification. The resulting framework is therefore not legally empty; rather, it is characterized by regulatory overlap that requires systematic interpretation.

The central legal problem emerges when an electronic medical record is compromised and the parties involved attempt to determine who is responsible. Consider a hospital whose database is infiltrated through stolen employee credentials, a ransomware attack, an improperly configured cloud server, or a vulnerability in an electronic medical-record platform. The hospital may argue that an external hacker caused the breach and that the institution therefore should not be considered responsible. A technology provider may similarly argue that the hospital controlled the system and failed to implement adequate security measures. An employee may be individually blamed for unauthorized access, even though the hospital may have failed to establish appropriate access controls, authentication systems, monitoring, or employee training. This illustrates why data-breach liability cannot be reduced to identifying the person who physically accessed or disclosed the information. The more fundamental legal question is whether the institution responsible for patient data exercised reasonable organizational control over the risks associated with that data. Contemporary healthcare cybersecurity literature supports this perspective because breaches frequently arise from combinations of technological vulnerabilities and human or organizational failures rather than from a single isolated act (Keshta and Odeh 2019; Kruse et al. 2017).

The problem is particularly important because electronic health information possesses a distinctive combination of sensitivity and utility. Healthcare providers require detailed information to diagnose and treat patients, coordinate referrals, conduct billing, satisfy regulatory requirements, and undertake public-health activities. At the same time, the same information can be exploited for purposes unrelated to healthcare. A patient's diagnosis of a communicable disease, mental-

health condition, infertility, cancer, genetic disorder, or substance-use disorder may have serious social consequences if disclosed without authorization. Gariйpy-Saper and Decarie's review of electronic-health-record privacy literature demonstrates that technological improvements have not eliminated longstanding concerns surrounding confidentiality, access, secondary use, and patient control (Gariйpy-Saper and Decarie 2021). The problem therefore cannot be solved merely by digitizing records and assuming that technical encryption will provide sufficient protection. Privacy is a legal and institutional obligation that must be embedded throughout the information lifecycle. Indonesian health law consequently needs to treat cybersecurity not simply as an information-technology issue but as an element of patient safety and institutional duty.

The adoption of electronic records also changes the scale and speed of potential harm. A paper record improperly viewed by one unauthorized employee may affect a single patient. A compromised database, however, can expose thousands or millions of records almost instantaneously. The expansion of health-information exchange can further increase exposure because records may move among hospitals, laboratories, pharmacies, insurers, government systems, and technology vendors. Empirical research indicates that greater electronic health-information exchange may increase certain categories of breach risk, particularly when information is shared externally and security practices are uneven across organizations (Li et al. 2023).

This means that the legal system must recognize networked responsibility. The hospital may not control every technological component involved in processing patient data, but it remains the institution through which patients receive healthcare and from which many data-processing activities originate. A legal framework that places responsibility exclusively on an external vendor or individual employee may therefore leave patients without an effective institutional remedy.

The Indonesian PDP Law provides an important foundation for resolving this problem because it adopts an accountability-oriented approach. Article 47 requires a personal-data controller to be responsible for the processing of personal data and to demonstrate accountability in fulfilling data-protection principles. Article 35 further requires the controller to protect and ensure the security of processed personal data through technical and operational measures and to determine the appropriate level of security by considering the nature and risks of the data.

These provisions are especially significant for hospitals because health information is expressly classified as specific personal data. The legal standard therefore cannot reasonably be limited to preventing intentional disclosure. It requires a broader assessment of whether the hospital implemented safeguards proportionate to the sensitivity and risks associated with health information. The concept of accountability consequently moves the analysis from “who leaked the data?” toward “who had the legal and organizational responsibility to prevent, detect, respond to, and remedy the failure?” This shift provides the foundation for a stronger institutional model of hospital liability.

The breach-notification mechanism reinforces this accountability orientation. Article 46 of the PDP Law requires a personal-data controller to provide written notification of a failure of personal-data protection no later than 3 Ч 24 hours to the affected data subject and the relevant institution, with information concerning the data disclosed, the timing and manner of disclosure, and mitigation and recovery measures.

This provision is important because breach response is itself a legally regulated activity. A hospital cannot satisfy its responsibilities merely by attempting to prevent breaches; once a failure occurs, the institution must also respond transparently and undertake appropriate recovery. Delay, concealment, or inadequate communication may aggravate the consequences of the original security failure. The notification requirement also recognizes that patients have an interest in knowing whether their health information has been compromised so that they can take appropriate protective measures. Accordingly, hospital liability should be assessed across the entire breach lifecycle: prevention, detection, containment, notification, recovery, and remediation. This article argues that this lifecycle approach offers a more coherent basis for interpreting Indonesian health and data-protection law.

The research gap addressed in this article concerns the relationship between health-sector confidentiality and general personal-data protection. Indonesian scholarship has increasingly examined the legal consequences of patient-data leakage and generally recognizes that hospitals bear substantial responsibility under the PDP Law and health regulations. However, significant questions remain concerning the precise basis, scope, and limits of institutional liability when a breach results from a complex interaction among hospital personnel, information-system vendors, cloud infrastructure, cybersecurity contractors, and external attackers. Existing Indonesian legal discussions also tend to focus on whether hospitals can be held responsible rather than developing a systematic framework for determining when, why, and to what extent such responsibility should arise. Recent Indonesian scholarship similarly identifies hospitals as potential personal-data controllers and recognizes administrative, civil, and criminal dimensions of responsibility, but the normative architecture connecting these forms of liability requires further development. The contribution of this article is therefore to reconstruct hospital liability around institutional risk control rather than individual fault alone.

This article employs a normative juridical methodology using statutory, conceptual, and comparative approaches. The statutory analysis focuses on Law Number 17 of 2023 concerning Health, Law Number 27 of 2022 concerning Personal Data Protection, Minister of Health Regulation Number 24 of 2022 concerning Medical Records, and Government Regulation Number 28 of 2024 concerning the implementation of the Health Law. PP No. 28 of 2024 functions as

an important implementing regulation within the contemporary health-law framework and was enacted on July 26, 2024.

Secondary materials include scholarly literature addressing electronic-health-record privacy, healthcare cybersecurity, institutional responsibility, and data-breach risk. Comparative analysis is used selectively to identify principles that may inform Indonesian legal development without mechanically importing foreign doctrines. The article advances the proposition that hospital liability should be reconstructed around five interconnected dimensions: institutional control, risk-based security, accountability for processors and vendors, breach-response obligations, and effective patient remedies. This framework seeks to preserve legal certainty while recognizing the technological complexity of modern healthcare information systems.

The article is organized into four substantive discussions. The first examines the legal status of electronic medical records and patient privacy under Indonesian health and data-protection law. The second analyzes the hospital as an institutional data controller and develops the normative basis for hospital liability. The third addresses responsibility within the healthcare data ecosystem, including employees, healthcare professionals, electronic-system providers, cloud-service vendors, and other processors. The fourth develops a risk-based model of hospital liability and considers remedies, breach notification, evidentiary issues, and regulatory reform. The central argument throughout is that the existence of an external cyberattack or an individual employee's misconduct should not automatically eliminate institutional responsibility. Where the hospital controls the infrastructure, policies, access architecture, vendor relationships, and data-processing environment, it occupies a privileged position to prevent foreseeable harm. Legal accountability should therefore follow organizational capacity to control risk, while remaining proportionate to the actual breach of duty and causal contribution.

Electronic Medical Records, Medical Confidentiality, and the Legal Status of Patient Data

Electronic medical records should be understood simultaneously as clinical instruments, legal documents, and repositories of personal information. Their primary function is to support healthcare delivery by recording patient identity, medical history, diagnoses, examinations, medications, laboratory findings, radiological results, treatment plans, and other relevant information. Yet the same information creates legal interests for the patient because it concerns the most intimate dimensions of individual life. Indonesian law reflects this dual character. Law Number 17 of 2023 recognizes the patient's right to obtain health information and access information contained in medical records while simultaneously requiring healthcare facilities to maintain the security, integrity, confidentiality, and availability of medical-record data.

The legal relationship is therefore not one in which the hospital possesses unlimited ownership over the patient's information. Rather, the institution has custody and governance responsibilities over information that remains closely connected to the patient's rights. This distinction is fundamental to determining liability because a hospital's legal obligations arise precisely from its position as the custodian and processor of sensitive information. Minister of Health Regulation Number 24 of 2022 strengthens this interpretation by expressly requiring healthcare facilities to implement electronic medical records and identifying security, confidentiality, integrity, and availability as core objectives of medical-record governance.

The regulation responds to the reality that healthcare digitalization creates risks that cannot be addressed through rules designed primarily for paper records. Electronic records can be copied without physical detection, transferred across networks, accessed remotely, integrated automatically with other systems, and processed through software that may involve multiple external service providers. Consequently, confidentiality must be supported by technical and organizational safeguards. A hospital that stores medical records electronically therefore assumes responsibilities concerning authentication, authorization, access logging, system integrity, backup, disaster recovery, data transmission, and user governance. The legal obligation to maintain confidentiality should thus be interpreted functionally: it requires institutions to establish conditions under which unauthorized access becomes reasonably difficult and unauthorized disclosure becomes reasonably detectable. The existence of an electronic system does not reduce the confidentiality obligation; instead, it expands the range of safeguards required to fulfill it.

The PDP Law adds another legal layer by expressly classifying health and health-information data as specific personal data. Article 4 states that specific personal data includes health and health-information data, biometric data, genetic data, criminal records, children's data, financial data, and other categories designated by law. The classification is important because the law recognizes that certain forms of personal information create greater risks to individuals than ordinary identifying information. Health information can be used to discriminate, stigmatize, manipulate, or otherwise harm individuals when improperly disclosed. Therefore, hospitals processing medical records cannot approach security as though they were protecting ordinary administrative information. The sensitivity of the data should influence the level of technical and organizational security implemented. This interpretation is consistent with Article 35, which requires controllers to determine security levels by considering the nature and risks of personal data processed. The statutory framework thus supports a risk-based interpretation rather than a uniform minimum-security approach.

The confidentiality obligation also extends beyond preventing deliberate publication. A breach may occur through unauthorized internal access, accidental disclosure, phishing, ransomware, stolen credentials, insecure application

programming interfaces, misconfigured cloud storage, lost devices, or inadequate disposal procedures. Empirical research demonstrates that human factors remain an important component of healthcare cybersecurity. An analysis of healthcare breaches found that a substantial portion of compromised records involved human security failures, with unintentional insider incidents producing significant numbers of affected records (Snyder et al. 2022).

This evidence is legally relevant because it challenges the assumption that cybersecurity responsibility belongs exclusively to information-technology departments. Employees operate within organizational systems established by hospitals. If staff members are granted excessive privileges, receive inadequate security training, use weak authentication, or are not subject to appropriate monitoring, the resulting vulnerability may reflect an institutional failure. The legal analysis should therefore distinguish individual misconduct from organizational conditions that made the misconduct possible.

The patient's privacy interest should also be distinguished from the hospital's operational interest in using medical information. Healthcare requires data sharing. A physician may need access to laboratory results generated elsewhere, a specialist may require referral information, and emergency personnel may need access to previous medical records. The legal objective cannot therefore be interpreted as absolute secrecy. Rather, the objective is controlled and lawful access. The PDP Law establishes principles including protection, legal certainty, public interest, benefit, prudence, balance, accountability, and confidentiality.

These principles indicate that data protection is intended to balance legitimate healthcare uses with individual rights. Consequently, a hospital may lawfully process patient data when a valid legal basis exists, but it remains obligated to ensure that processing is limited to legitimate purposes and protected against unauthorized access. Privacy protection should therefore be understood as governance of access rather than prohibition of data use. This distinction becomes crucial when evaluating whether a particular disclosure or system integration constitutes a breach.

The legal significance of medical-record confidentiality is further reinforced by professional obligations. Law Number 17 of 2023 establishes that medical personnel and health workers must preserve the confidentiality of patients' personal health information in the performance of healthcare services. This creates an individual professional duty that coexists with the hospital's institutional duties. A physician who intentionally accesses or discloses information unrelated to patient care may therefore bear personal responsibility. Yet the existence of professional confidentiality cannot be used to shift all cybersecurity responsibility onto individual clinicians. The hospital controls the technological architecture within which clinicians operate. If every employee can access every patient's record without role-based restrictions, the problem is not merely that employees possess insufficient ethical discipline; the institution may have created an inappropriate access environment. Professional confidentiality and institutional security must

therefore operate together. A robust legal framework recognizes both levels rather than allowing one to substitute for the other.

This distinction becomes particularly important when an employee accesses the medical record of a celebrity, public official, colleague, or acquaintance without a legitimate clinical reason. The individual employee may have committed a clear confidentiality violation. However, institutional responsibility depends on whether the hospital had reasonable safeguards to prevent, detect, and respond to such access. De Simone's analysis of unauthorized medical-record access demonstrates that improper access by healthcare workers is a significant privacy concern and may carry legal consequences beyond internal disciplinary action (De Simone 2019). If a hospital maintains effective role-based access, audit trails, anomaly detection, and disciplinary procedures, individual misconduct may be more appropriately attributed to the employee. If the hospital provides unrestricted access and does not monitor activity, the institution's responsibility becomes stronger. This distinction reflects the principle that liability should correspond not merely to the immediate actor but also to the organizational environment that enabled the breach.

The confidentiality of medical records should also be considered in relation to patient autonomy. Privacy allows individuals to decide when and with whom information concerning their bodies, illnesses, and treatment is shared. A breach can therefore interfere with autonomy even when no direct financial loss occurs. Gariйpy-Saper and Decarie (2021) note that electronic health-record privacy involves multiple perspectives, including those of patients, healthcare professionals, information specialists, and institutions, and that technological development does not eliminate the underlying ethical tensions surrounding access and confidentiality. Indonesian law should similarly avoid defining harm solely in economic terms. The disclosure of a sensitive diagnosis may produce reputational or psychological consequences that are difficult to quantify. A patient-protection framework must therefore recognize privacy as an independent legal interest. This strengthens the argument that hospital liability should encompass breaches of confidentiality even where the patient cannot demonstrate conventional financial loss.

The Hospital as Institutional Data Controller and the Basis of Liability

The most important conceptual question is whether a hospital should be treated as an institutional data controller when it operates an electronic medical-record system. Under the PDP Law, the controller is the party that determines the purpose and exercises control over personal-data processing. Hospitals that determine why patient information is collected, how it is used in healthcare delivery, who may access it, how long it is retained, and which systems or vendors process it will ordinarily occupy a central position in this legal relationship. The precise

classification may depend on the institutional arrangement, particularly where government systems, independent physicians, laboratories, or external technology providers participate. Nevertheless, in ordinary hospital-based care, the institution is the actor best positioned to determine the architecture through which patient data are governed. Article 47's accountability principle is therefore particularly relevant because it places responsibility on the controller to demonstrate compliance rather than simply asserting that another party caused the breach. This shifts the legal analysis from reactive blame toward demonstrable institutional compliance. Article 35 of the PDP Law provides a particularly strong foundation for hospital responsibility because it expressly requires controllers to protect and ensure the security of processed personal data. The provision requires technical and operational measures to prevent unlawful processing and requires security levels to be determined according to the nature and risks of the data.

For healthcare institutions, the implication is significant. Hospitals should be expected to undertake security measures proportionate to the sensitivity and scale of their information systems. The relevant safeguards may include access controls, strong authentication, encryption, network segmentation, vulnerability management, backup systems, employee training, incident-response plans, logging, monitoring, and periodic security assessments. The law does not necessarily require every hospital to implement identical technologies. A small clinic and a large tertiary hospital may face different risks and possess different resources. However, both should be able to demonstrate that security measures correspond to their actual risk environment. The legal standard should therefore be one of reasonable and risk-proportionate security rather than technological perfection.

The institutional nature of hospital liability becomes clearer when cybersecurity is considered as a patient-safety issue. A ransomware attack that locks a hospital's electronic records can affect not only privacy but also the continuity of healthcare. Clinicians may be unable to access medication histories, allergies, diagnostic results, or treatment records. Delayed access can therefore create clinical risks in addition to privacy harms. Digital-health scholarship increasingly recognizes that cybersecurity incidents can affect the safety and continuity of healthcare services rather than merely the confidentiality of information (Argaw et al. 2020; Coventry and Branley 2018). The legal consequence is that hospitals should treat cybersecurity governance as part of their general duty to provide safe healthcare. A hospital that fails to maintain adequate backup and recovery systems may create risks even if no patient data are ultimately disclosed. Conversely, an institution that experiences a sophisticated attack despite reasonable safeguards should not automatically be considered negligent. This distinction again supports a risk-based approach: liability should turn on whether the institution exercised reasonable preventive and responsive measures, not simply on the occurrence of a breach.

Institutional control is especially important because hospitals make decisions that individual clinicians cannot make. Hospital management determines which

electronic medical-record vendor to use, whether data are stored on-premises or through cloud services, how user privileges are structured, what cybersecurity budget is allocated, which vendors receive access to patient information, and whether security incidents are investigated. These are organizational decisions. A physician may be able to protect a password, but the physician cannot redesign the hospital's authentication architecture. A nurse may comply with confidentiality rules, but cannot determine whether the hospital encrypts its database. A receptionist may accidentally open a phishing email, but the institution controls employee training and endpoint security. Therefore, a legal framework that focuses exclusively on individual employee negligence fails to recognize the distribution of actual control. Institutional liability is justified precisely because hospitals possess the organizational capacity to establish systems that reduce the likelihood and impact of human error.

The hospital's responsibility also includes vendor governance. Modern healthcare institutions frequently depend on external providers for electronic-record software, cloud hosting, cybersecurity, data analytics, telecommunications, maintenance, and technical support. Outsourcing does not necessarily transfer the hospital's legal responsibility to the vendor. The PDP Law expressly contemplates relationships between personal-data controllers and processors, and Article 37 requires the controller to supervise parties involved in processing personal data under its control.

This is crucial because hospitals cannot simply argue that an external vendor caused the breach and therefore the hospital bears no responsibility. If the hospital selected a vendor without assessing security capabilities, failed to establish contractual security requirements, granted excessive access, or neglected vendor monitoring, institutional responsibility may arise. Conversely, where a hospital conducts reasonable due diligence and the vendor independently commits a serious security failure contrary to contractual and technical requirements, liability may be allocated differently. Vendor outsourcing therefore requires governance rather than automatic transfer of responsibility.

The supervisory obligation toward processors is especially important because patient data may travel through several layers of technological infrastructure. A hospital may contract with an electronic-record vendor that relies on a cloud provider, which may itself depend on data centers, cybersecurity services, and subcontractors. From the patient's perspective, however, these distinctions may be invisible. The patient typically provides information to the hospital for healthcare purposes, not to a chain of commercial technology companies. The legal system should therefore prevent excessive fragmentation of responsibility. Hospitals should remain accountable for choosing and supervising processors within their data-processing ecosystem. This does not mean that processors are immune from direct responsibility. Rather, it means that the hospital's duty to patients cannot be eliminated merely through contractual outsourcing. The institutional accountability model is therefore compatible with contractual allocation of risk among

commercial actors while preserving the patient's ability to seek a remedy from the healthcare institution that controlled the primary data relationship.

Hospital liability should also be analyzed through the distinction between strict liability and negligence-based liability. A strict-liability model would make hospitals responsible whenever a breach occurs, regardless of whether reasonable security measures were implemented. Such an approach would provide strong patient protection but may be excessively burdensome because sophisticated cyberattacks can defeat even advanced security systems. A negligence-based model, by contrast, requires proof that the hospital failed to satisfy an applicable duty. This is more consistent with traditional legal reasoning but may create evidentiary difficulties for patients who cannot access internal security records. The preferable approach is a risk-based negligence model supplemented by accountability and disclosure obligations. Under this model, a breach does not automatically establish liability, but the hospital must be able to demonstrate reasonable compliance with security obligations. Where a hospital cannot produce evidence of basic safeguards, the evidentiary consequences should weigh against the institution. This approach avoids absolute liability while recognizing that hospitals possess substantially greater access to relevant information.

The standard of reasonable security should be dynamic. Cybersecurity practices that were adequate several years ago may become insufficient as attack techniques evolve. Therefore, hospitals should not be able to rely indefinitely on historical compliance. The statutory requirement in Article 35 to determine security levels according to the nature and risks of personal data supports an adaptive interpretation. A hospital processing millions of records through an interconnected digital infrastructure should reasonably face a higher governance expectation than an institution maintaining a small and isolated database. Similarly, hospitals handling highly sensitive specialist data may require stronger safeguards. This risk-sensitive approach is consistent with cybersecurity literature showing that healthcare organizations face changing threats and that security depends on both technical and organizational factors (Kruse et al. 2017; Keshta and Odeh 2019). The law should therefore assess whether the hospital's security posture was reasonable in light of the foreseeable risks at the time of the breach, rather than asking whether the institution possessed perfect protection.

Article 46 of the PDP Law further establishes an independent obligation concerning breach response. When a failure of personal-data protection occurs, the controller must provide written notification within 3 Ч 24 hours to the data subject and the relevant institution, including information concerning the affected data, when and how the failure occurred, and the mitigation and recovery measures undertaken. This requirement transforms incident response from a discretionary public-relations decision into a legal obligation. A hospital therefore has a duty not only to investigate internally but also to communicate relevant information to affected patients and authorities within the prescribed period. The quality of notification is important because vague statements may prevent patients from

understanding the nature of the risk. A meaningful notice should allow patients to determine what categories of health information may have been exposed and what protective steps are appropriate. Failure to comply with notification requirements should consequently be considered a separate component of institutional non-compliance.

The accountability principle under Article 47 provides an additional basis for requiring hospitals to demonstrate their compliance. Accountability is stronger than a general obligation to behave responsibly because it implies the ability to demonstrate that appropriate systems were established and operated. For hospitals, this could involve maintaining cybersecurity policies, access-control records, risk assessments, training documentation, vendor contracts, security audits, incident logs, and evidence of corrective actions. Such documentation serves two functions. First, it facilitates regulatory supervision and continuous improvement. Second, it provides evidence in legal disputes concerning whether the hospital exercised reasonable care. The absence of documentation should therefore be legally significant because a hospital cannot credibly demonstrate accountability if it cannot show what security measures were implemented. This is particularly important where patients face an informational disadvantage. Without access to institutional records, patients may know that a breach occurred but be unable to establish why it occurred. Accountability mechanisms can help correct that asymmetry.

Allocation of Responsibility among Hospitals, Healthcare Workers, and Technology Providers

Although hospitals occupy a central position, they are not the only actors within the electronic medical-record ecosystem. Physicians, nurses, administrative employees, information-technology personnel, electronic-record vendors, cloud providers, cybersecurity contractors, and other processors may all interact with patient data. A coherent legal framework must therefore avoid treating the hospital as automatically liable for every event regardless of its cause. The appropriate approach is differentiated responsibility based on control, duty, foreseeability, and causal contribution. A healthcare worker who intentionally sells patient data should not be shielded merely because the hospital employs that person. Similarly, a technology provider that introduces a serious security vulnerability should not escape responsibility merely because its customer is a hospital. The objective is therefore not to replace individual liability with institutional liability but to establish a layered structure in which each actor is responsible for risks within its sphere of control. This model is consistent with contemporary data-protection governance, which distinguishes controllers and processors while requiring appropriate supervision and accountability across the processing chain.

Healthcare professionals have a direct ethical and legal duty to preserve patient confidentiality. Their responsibility becomes particularly relevant where the

breach results from deliberate or careless access. Examples include viewing records of patients without a clinical purpose, sharing screenshots through personal messaging applications, downloading records to unsecured devices, or discussing identifiable patient information outside legitimate professional contexts. Such conduct may constitute individual misconduct regardless of the hospital's broader cybersecurity system. However, the existence of individual responsibility does not necessarily eliminate institutional responsibility. If the hospital failed to establish role-based permissions, allowed employees to access large numbers of unrelated patient records, or did not maintain audit logs, the institutional environment may have materially contributed to the breach. The correct legal inquiry should therefore examine both the employee's conduct and the hospital's governance. This prevents the common error of treating employee misconduct as an automatic defense for the institution. An organization remains responsible for creating and maintaining a secure environment in which employees operate.

The hospital's relationship with technology providers presents a more difficult allocation problem. Electronic medical-record vendors may design and maintain the software architecture, while hospitals determine how the system is configured and used. A breach may therefore result from a vulnerability in the vendor's software, a hospital's configuration, or both. The legal framework should distinguish these scenarios. If a vendor knew or reasonably should have known about a serious vulnerability and failed to patch or disclose it, the vendor may bear direct responsibility. If the hospital ignored available security updates or configured the system contrary to the vendor's recommendations, hospital responsibility may become stronger. If both actors materially contributed, concurrent responsibility should be possible. The objective is to avoid a simplistic assumption that software vendors are always responsible for software vulnerabilities or that hospitals are always responsible because they operate the system. Liability should instead follow the actor's control over the relevant risk.

Cloud computing further complicates this relationship because hospitals may not physically possess the servers on which patient information is stored. Physical custody, however, should not be confused with legal control. A hospital may still determine the purposes of processing, authorize access, select the cloud provider, determine retention periods, and decide which information is transferred to the cloud environment. The fact that a third party physically stores the data does not automatically eliminate the hospital's responsibilities as controller. At the same time, cloud providers may possess independent technical responsibilities concerning infrastructure security. The legal system should therefore recognize a layered model. The hospital remains responsible for governance of the data relationship, while the cloud provider may be responsible for infrastructure-level security failures within its contractual and technical control. This approach mirrors broader accountability principles in data-protection law and prevents contractual arrangements from obscuring responsibility.

The hospital's procurement decisions are particularly important. A hospital that selects an electronic medical-record system should conduct reasonable due diligence concerning security features, vendor reputation, vulnerability management, encryption, authentication, incident-response capabilities, data location, subcontracting arrangements, and update procedures. A procurement process focused exclusively on cost or functionality may create foreseeable security risks. The legal relevance of procurement is that it occurs before the breach and therefore represents an opportunity for prevention. If a hospital selects a system known to have significant security deficiencies without implementing compensating safeguards, subsequent liability may be stronger. Conversely, a hospital that selects a reputable provider, conducts appropriate assessments, implements recommended safeguards, and continuously monitors the system may have a stronger defense against negligence claims when confronted by an unforeseeable attack. Procurement should therefore be understood as a component of the hospital's duty of care rather than a purely commercial decision.

Vendor contracts should also establish clear obligations concerning security, access, incident reporting, vulnerability disclosure, audit rights, subcontracting, data deletion, and cooperation with investigations. However, contracts should not be permitted to eliminate patient rights. A hospital may agree with a technology vendor that the vendor will indemnify the hospital for certain losses, but such an arrangement should operate primarily between the commercial parties. The patient did not negotiate the contract and should not bear the consequences of contractual provisions that make recovery practically impossible. This distinction is important for the development of a patient-centered liability system. Private allocation of financial risk can determine which commercial actor ultimately bears the cost, but it should not determine whether the patient can seek a legal remedy. The hospital may subsequently seek contribution from the vendor if the vendor caused or contributed to the breach. This allows commercial risk allocation while preserving the patient's substantive protection.

An additional issue concerns cybersecurity standards and the meaning of “reasonable security.” Indonesian law establishes the obligation but does not necessarily prescribe one exhaustive technical standard applicable to every hospital. This creates flexibility but also uncertainty. The legal system can address the problem by considering recognized technical standards, sectoral guidance, security assessments, professional practices, and the actual risk profile of the institution. Courts should avoid treating compliance with a particular technical certification as conclusive proof of non-liability or, conversely, treating the absence of certification as automatic negligence. Cybersecurity is dynamic, and formal certification may not capture every relevant risk. Nevertheless, recognized standards can provide evidence of what reasonable organizational security requires. The legal standard should remain outcome-independent: a breach does not necessarily prove negligence, and the absence of a breach does not necessarily

prove compliance. Instead, the focus should remain on whether the institution implemented reasonable safeguards before the incident.

The allocation of responsibility should also recognize the difference between malicious external attacks and preventable internal failures. A sophisticated zero-day attack that defeats reasonable security measures presents a different legal situation from a breach caused by a hospital's failure to disable former employees' accounts. The first may be difficult to attribute to hospital negligence; the second may provide strong evidence of institutional failure. Similarly, a phishing attack against an employee should not automatically be considered the employee's fault if the institution provided no cybersecurity training or multifactor authentication. Human behavior is embedded within technical and organizational systems. Research on healthcare breaches demonstrates that employee behavior can significantly influence the likelihood and scale of incidents (Snyder et al. 2022).

Therefore, hospitals should be expected to design systems that anticipate foreseeable human error rather than relying exclusively on employee vigilance. A risk-based allocation can be represented through five categories of responsibility as shown on Table 1.

TABLE 1. Five Categories of Responsiblity Electronic Medical Records

Actor	Principal Control	Relevant Duty	Potential Failure	Liability Orientation
Hospital	Institutional governance	Secure processing and patient protection	Weak security, poor access controls, inadequate vendor governance	Primary institutional liability
Physician/Health Worker	Professional access and use	Confidentiality and lawful access	Unauthorized access/disclosure	Individual professional/civil liability
EMR Vendor	Software design and maintenance	Secure system architecture and vulnerability management	Software vulnerability, inadequate security update	Contractual/civil liability
Cloud/IT Provider	Infrastructure and technical environment	Infrastructure security and availability	Server compromise, misconfiguration	Contractual/civil liability
Processor/ Subprocessor	Specific processing activity	Compliance with controller instruction		

Source: Various sources, edited and analyzed by Author

This structure (Table 1) illustrates why the hospital should be regarded as the central but not exclusive locus of accountability. The hospital is normally the institution that establishes the patient relationship, determines the primary purposes of processing, selects or authorizes technology, manages users, and integrates medical records into clinical workflows. Yet other actors may exercise specialized

control over particular risks. Liability should therefore be allocated according to the specific breach rather than imposed mechanically. This approach also has an important preventive function because it creates incentives for each participant to improve the security of its own operations. A vendor cannot assume that the hospital will absorb all risk, while a hospital cannot assume that outsourcing transfers all responsibility. Similarly, employees remain subject to confidentiality obligations while hospitals remain responsible for designing organizational systems that reduce foreseeable misuse.

A Risk-Based Framework for Hospital Liability, Remedies, and Legal Reform

A coherent framework for hospital liability should begin with the proposition that a data breach is not itself sufficient to establish legal fault. Digital systems operate under conditions of uncertainty, and even sophisticated security systems may be defeated by highly capable attackers. Automatic liability could therefore produce excessive risk transfer to hospitals and potentially discourage digital innovation. At the same time, requiring patients to prove every technical detail of a cybersecurity failure would create an unfair evidentiary burden because the relevant information is usually controlled by the hospital and its technology providers. The appropriate solution is a risk-based accountability framework that combines substantive duties with procedural transparency. Under this framework, liability should be assessed according to the sensitivity of the data, scale of processing, foreseeable threats, security measures implemented, institutional control, breach response, and causal relationship between the security failure and the harm suffered. This model is consistent with Article 35's requirement that security measures reflect the nature and risks of the personal data involved.

The first element should be risk identification and prevention. Hospitals should conduct periodic assessments of threats affecting electronic medical records, including unauthorized access, credential theft, malware, ransomware, insider misuse, insecure interfaces, third-party vulnerabilities, and physical compromise of devices. Risk assessment should not be a one-time administrative exercise. It should be repeated when systems change, new vendors are introduced, data are transferred to new environments, or significant cybersecurity threats emerge. A hospital's failure to conduct any meaningful risk assessment may indicate institutional negligence because the law expressly requires security measures to be proportionate to the nature and risks of the data. The hospital should also establish policies concerning access privileges, password management, multifactor authentication, encryption, data retention, backups, mobile devices, remote access, and incident reporting. These measures do not guarantee that a breach will never occur. Their legal purpose is to demonstrate that the institution took reasonable steps to prevent foreseeable harm.

The second element should be access governance. Not every employee requires access to every medical record. Role-based access should restrict users to information necessary for legitimate professional functions. Audit logs should record significant access events and permit investigation of suspicious activity. Particularly sensitive records may require additional authorization. Access should also be reviewed when employees change roles or leave the institution. Such measures are legally important because unauthorized access is one of the most common mechanisms through which confidentiality can be compromised. If a hospital gives broad access without legitimate operational justification, it increases foreseeable risk. Conversely, an employee who deliberately circumvents reasonable access controls may bear substantial individual responsibility. The legal framework should therefore assess both the institutional design and the individual's conduct. The objective is to create a system in which unauthorized access is difficult, detectable, and subject to appropriate consequences.

The third element should be technical and organizational security. Technical measures may include encryption at rest and in transit, secure authentication, endpoint protection, vulnerability management, network segmentation, intrusion detection, secure software development, backups, and disaster-recovery systems. Organizational measures include employee training, cybersecurity governance, incident-response teams, policies, audits, vendor oversight, and executive accountability. Literature on healthcare cybersecurity emphasizes that technical solutions alone are insufficient because security depends on human behavior, organizational culture, and governance (Keshta and Odeh 2019; Kruse et al. 2017). This principle is particularly relevant in Indonesia because hospitals vary significantly in technological capacity. The legal standard should not require every institution to possess identical infrastructure, but it should require each institution to implement safeguards proportionate to its size, data volume, technological dependence, and threat environment. Resource limitations may be relevant to assessing reasonableness, but they should not become a blanket justification for failing to protect highly sensitive information.

The fourth element should be vendor and processor governance. Before transferring patient data to an external provider, a hospital should assess the provider's security architecture, contractual commitments, incident history, subcontracting arrangements, access privileges, data location, and ability to respond to security incidents. Contracts should establish security standards and require prompt notification of suspected breaches. Hospitals should also retain sufficient audit rights to verify compliance. This approach is important because healthcare data breaches increasingly occur across interconnected networks rather than within a single institution. Research examining health-information exchange suggests that external information sharing can increase long-term breach risk and that security may be constrained by the weakest link in the information-sharing ecosystem (Li et al. 2023). Hospital responsibility should therefore include

reasonable oversight of external processors. Outsourcing may distribute technical tasks, but it should not eliminate governance responsibility.

The fifth element should be incident response and breach notification. Once a hospital discovers a data-security incident, it should immediately activate an incident-response procedure designed to contain the breach, preserve evidence, determine its scope, restore systems, and protect affected patients. Article 46 of the PDP Law imposes a specific notification deadline of 3 Ч 24 hours and identifies minimum information that must be communicated. The legal significance of this provision is that the response itself becomes part of accountability. A hospital that initially experiences an attack but rapidly detects, contains, investigates, and reports the incident may have acted reasonably even if some data were compromised. Conversely, an institution that discovers a breach but delays notification, destroys relevant evidence, or minimizes the scope of the incident may create additional legal exposure. The quality of response should therefore influence the assessment of institutional responsibility.

The sixth element should be patient remedies. Privacy protection is incomplete if patients possess rights but lack effective mechanisms for compensation and redress. The PDP Law establishes rights for data subjects and provides a framework for administrative, civil, and criminal consequences in specified circumstances. The health-law framework also recognizes patient rights concerning information and medical records. Remedies should reflect the nature of the harm. Where a breach causes direct financial loss, compensation may be relatively straightforward. However, privacy injuries may involve distress, reputational damage, discrimination, or exposure of highly sensitive medical information that is difficult to monetize. Indonesian legal development should therefore recognize that unauthorized disclosure of sensitive health information may constitute a legally meaningful injury even where conventional economic damage is difficult to establish. This would strengthen the protective function of data-protection law.

An important evidentiary issue arises because patients typically do not possess information necessary to prove a hospital's security failure. A patient may know that medical records were leaked but not whether the breach resulted from weak encryption, stolen credentials, inadequate patching, employee misconduct, vendor negligence, or a sophisticated external attack. The hospital and its vendors, by contrast, may possess logs, audit reports, incident-response records, security assessments, and contractual documentation. This asymmetry justifies greater procedural disclosure obligations. Where a patient establishes that the hospital controlled the relevant records, a breach occurred, and the patient's data were affected, the hospital should be required to produce relevant security and incident records subject to legitimate confidentiality and trade-secret protections. This does not create automatic liability. Instead, it allows the court to assess whether the institution complied with its statutory obligations. Such an approach is particularly

compatible with Article 47's accountability principle because the controller is expressly required to demonstrate responsibility for compliance.

The evidentiary model should also distinguish between the occurrence of a breach and the cause of a breach. A hospital may legitimately argue that an attack was sophisticated and unforeseeable. But such an argument should be evaluated against evidence of the hospital's security posture. If the institution maintained appropriate safeguards, updated its systems, monitored access, trained employees, and implemented incident response, the breach may not establish negligence. If, however, the institution failed to apply basic security updates for an extended period, allowed former employees to retain access, used shared administrator accounts, or failed to monitor obvious vulnerabilities, the attacker's role should not automatically absolve the hospital. The existence of a malicious third party does not necessarily break legal causation where the institution's negligence materially enabled the harm. This causal approach prevents cybersecurity incidents from becoming an area of automatic immunity.

The framework should further distinguish between privacy harm and clinical harm. A data breach may expose health information without affecting the patient's medical treatment. Conversely, a cyberattack may disrupt access to medical records and thereby contribute to a clinical injury. These situations involve different causal pathways. In the first, liability concerns confidentiality and data protection. In the second, the same security failure may also implicate the hospital's duty to provide safe and continuous healthcare. The distinction is important because the appropriate remedy and standard of causation may differ. A patient whose diagnosis was publicly disclosed may seek compensation for privacy-related harm even if treatment remained unaffected. A patient who suffered medical injury because ransomware made critical records unavailable may potentially assert a separate healthcare liability claim. Digital healthcare law should therefore avoid collapsing all cyber incidents into a single legal category.

The principle of proportionality should govern allocation among multiple responsible parties. If a hospital failed to conduct vendor due diligence while a vendor independently introduced a serious vulnerability, both may have contributed to the harm. The hospital may be responsible for inadequate governance, while the vendor may be responsible for the technical defect. If an employee intentionally sells records despite robust institutional controls, the employee may bear primary responsibility. If the hospital failed to implement even basic access restrictions, institutional responsibility becomes stronger. Proportionality allows the legal system to distinguish these cases. It also encourages contribution and indemnification mechanisms among commercial actors. The patient should not be required to resolve the internal contractual allocation before obtaining a remedy. Once the patient's legal entitlement is established, the responsible institutions can determine contribution according to their respective causal and contractual positions.

Comparative experience reinforces the value of an institutional approach. In the United States, for example, healthcare privacy regulation places substantial responsibility on healthcare organizations for protecting protected health information and managing relationships with business associates. Research examining electronic sharing under HIPAA demonstrates that the recipient organization generally assumes responsibility for safeguarding information within its control, including through business associates (Cohen et al. 2020). Indonesia should not simply transplant HIPAA because its statutory structure and institutional context differ. Nevertheless, the underlying principle is useful: organizations cannot evade responsibility merely because patient information passes through interconnected technological actors. Accountability should remain connected to organizational control over the information environment.

International health governance also supports the proposition that privacy and security are fundamental elements of digital-health governance. WHO's 2021 guidance emphasizes that privacy and confidentiality must be protected in AI and digital-health environments and identifies responsibility and accountability as core principles for health technology governance (World Health Organization 2021). This principle is applicable beyond artificial intelligence because electronic medical records constitute the foundational data infrastructure upon which many digital-health technologies depend. A healthcare system cannot credibly claim to be patient-centered while treating confidentiality as an optional technical feature. Privacy should instead be integrated into the design, procurement, deployment, and monitoring of digital systems. Indonesian law already contains the normative ingredients for this approach; what remains necessary is a coherent interpretation that connects those obligations to institutional accountability.

A further reform should concern privacy and security by design. Hospitals should incorporate data-protection requirements before deploying new electronic medical-record systems rather than treating security as a remedial concern after implementation. This approach is consistent with the risk-based logic of Article 35 and the broader principle that technical and organizational safeguards should correspond to data sensitivity. New systems should undergo security assessment before deployment, significant changes should trigger reassessment, and high-risk processing should receive heightened scrutiny. Hospitals should also establish governance committees capable of reviewing cybersecurity, privacy, clinical safety, and vendor risks together. Such governance is particularly important because digital systems can affect multiple legal interests simultaneously. A cybersecurity vulnerability may threaten privacy, healthcare continuity, professional confidentiality, and institutional reputation. Fragmented governance can therefore leave important risks unmanaged.

Another important reform concerns incident documentation and auditability. A hospital should maintain sufficient records to reconstruct significant security incidents, including relevant access logs, system events, notifications, vendor communications, and remedial actions. Documentation serves both accountability

and learning. Without reliable records, hospitals may be unable to identify whether similar vulnerabilities exist elsewhere in the system. It also becomes difficult for regulators or courts to determine whether the hospital acted reasonably. The requirement should not be interpreted as an obligation to retain unlimited personal data indefinitely because retention itself creates privacy risks. Rather, hospitals should maintain security-related evidence for appropriate periods consistent with medical-record retention and data-protection principles. The objective is to create traceability without encouraging unnecessary accumulation of sensitive information.

The regulatory framework should also clarify the relationship between the PDP Law and health-specific rules. The existence of multiple statutes can create uncertainty regarding which authority, remedy, or standard applies to a particular incident. Health law governs medical records and professional confidentiality, while the PDP Law governs personal-data processing. These regimes should be interpreted as complementary rather than mutually exclusive. Where a medical-record breach involves personal-data processing, both the healthcare-specific confidentiality framework and general data-protection obligations may apply. This dual applicability is not inherently problematic. Indeed, it can strengthen patient protection by addressing different dimensions of the same conduct. The challenge is ensuring that institutions understand their overlapping duties and that patients can identify the appropriate mechanisms for obtaining remedies. Regulatory guidance should therefore clarify the respective roles of health authorities and personal-data regulators.

The absence of a fully integrated enforcement architecture could otherwise produce fragmented accountability. A patient may be required to pursue one process concerning medical confidentiality, another concerning personal-data protection, and potentially another concerning civil compensation. Fragmentation increases the cost of enforcement and may discourage legitimate claims. The legal system should therefore consider mechanisms for coordinated investigation and remedy. Hospitals should have a clear internal complaint mechanism for data breaches, patients should receive information about available remedies, and regulators should coordinate where incidents implicate both health law and personal-data law. The goal should be to make accountability practically accessible rather than merely formally available. Patient protection is meaningful only if individuals can understand who is responsible, what rights they possess, and how they can obtain redress.

The ultimate normative basis for institutional hospital liability is therefore not simply the hospital's ability to pay compensation. It is the hospital's capacity to prevent and control risk. Hospitals are uniquely situated because they determine how patient information enters, moves through, and exits their organizational environment. They select technologies, establish policies, employ personnel, authorize access, contract with vendors, and respond to incidents. This combination of authority and capacity justifies placing the hospital at the center of

legal accountability. At the same time, institutional responsibility must remain proportionate and should not become absolute liability. Where a hospital can demonstrate that it implemented reasonable, risk-appropriate safeguards and that the breach resulted from an extraordinary event outside its reasonable control, liability may be reduced or excluded depending on applicable law. The central principle should therefore be: the greater the institutional control over a data-processing risk, the greater the corresponding duty to prevent, detect, and remedy that risk.

Conclusion

The digitalization of medical records has transformed patient privacy from a predominantly interpersonal confidentiality issue into a complex institutional and technological governance problem. Indonesian law already provides significant normative foundations for protecting electronic medical records. Law Number 17 of 2023 recognizes patient rights to health information and access to medical-record information while requiring healthcare facilities to maintain the security, integrity, confidentiality, and availability of medical-record data. Minister of Health Regulation Number 24 of 2022 establishes the mandatory electronic medical-record framework and expressly emphasizes security and confidentiality. Meanwhile, Law Number 27 of 2022 classifies health information as specific personal data, imposes security and confidentiality duties on controllers, establishes accountability, and requires breach notification within 3 Ч 24 hours. The principal legal challenge is therefore not the complete absence of regulation but the fragmentation of obligations across health, medical-record, and personal-data regimes. This fragmentation becomes especially problematic when breaches involve multiple actors, including hospitals, healthcare professionals, technology providers, cloud-service providers, and other processors.

This article argues that hospital liability should be reconstructed through a risk-based institutional accountability framework. A hospital should not be automatically liable merely because a cyberattack occurred, but neither should it be able to avoid responsibility by attributing the incident to an external hacker, employee, or technology vendor. Liability should depend on institutional control, foreseeable risk, adequacy of preventive safeguards, vendor governance, access management, breach response, and causal contribution. Hospitals should be expected to demonstrate reasonable security measures proportionate to the sensitivity and scale of the patient information they process. Healthcare professionals remain independently responsible for unlawful access and disclosure, while technology providers and processors should bear responsibility for risks within their technical and contractual control. Where several actors materially contribute to a breach, concurrent and proportionate liability should be available. The objective is not to impose strict liability on hospitals but to ensure that legal responsibility follows the actor most capable of preventing the relevant harm. Such

an approach would make patient privacy a substantive component of healthcare governance rather than a merely formal confidentiality obligation.

The framework should further strengthen breach notification, evidence preservation, auditability, patient remedies, and regulatory coordination. Article 46 of the PDP Law already establishes a 3 Ч 24-hour notification requirement, but effective implementation requires hospitals to maintain incident-response systems capable of identifying and documenting breaches promptly.

Patients should have meaningful access to information about the nature of the breach and the remedies available to them, while courts and regulators should have sufficient access to security records to assess institutional compliance. Ultimately, cybersecurity should be understood as part of patient safety and health justice. The protection of electronic medical records is not simply a technical responsibility delegated to information-technology departments; it is an institutional legal obligation arising from the hospital's role as healthcare provider, custodian of medical information, and central participant in the personal-data processing ecosystem. Strengthening institutional accountability would allow Indonesia to preserve the benefits of digital healthcare while ensuring that technological progress does not come at the expense of the fundamental privacy rights of patients.

References

Abouelmehdi, Karim, Abderrahim Beni-Hessane, and Hayet Khaloufi. 2018. "Big Healthcare Data: Preserving Security and Privacy." Journal of Big Data 5: 1–18. https://doi.org/10.1186/s40537-018-0110-7.

Al-Issa, Yara, Mustafa A. Ottom, and Ahmed Tamrawi. 2019. "eHealth Cloud Security Challenges: A Survey." Journal of Healthcare Engineering 2019: 1–15. https://doi.org/10.1155/2019/7516035.

Argaw, Seleshi T. et al. 2020. "Cybersecurity of Hospitals: A Systematic, Organizational Perspective." BMC Medical Informatics and Decision Making 20.

Cohen, I. Glenn, et al. 2020. "Doctors Routinely Share Health Data Electronically under HIPAA, and Sharing with Patients and Patients' Third-Party Health Apps Is Consistent: Interoperability and Privacy Analysis." Journal of Medical Internet Research 22 (9): e19818.

Coventry, Lynne, and Yvonne Branley. 2018. "Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward." Maturitas 113: 48–52.

De Simone, Donna M. 2019. "When Is Accessing Medical Records a HIPAA Breach?" Journal of Nursing Regulation 10 (3): 34. https://doi.org/10.1016/S2155-8256(19)30146-2.

Gariépy-Saper, Katherine, and Nicholas Decarie. 2021. "Privacy of Electronic Health Records: A Review of the Literature." Journal of the Canadian Health Libraries Association 42 (1). https://doi.org/10.29173/jchla29496.

Indonesia. 2022. Law Number 27 of 2022 concerning Personal Data Protection. State Gazette of the Republic of Indonesia 2022, No. 196.

Indonesia. 2022. Regulation of the Minister of Health Number 24 of 2022 concerning Medical Records.

Indonesia. 2023. Law Number 17 of 2023 concerning Health. State Gazette of the Republic of Indonesia 2023, No. 105.

Indonesia. 2024. Government Regulation Number 28 of 2024 concerning Implementing Regulations of Law Number 17 of 2023 concerning Health. State Gazette of the Republic of Indonesia 2024, No. 135.

Keshta, Ismail, and Alaa Odeh. 2019. "Security and Privacy of Electronic Health Records: Concerns and Challenges." Egyptian Informatics Journal 22 (2): 177–183. https://doi.org/10.1016/j.eij.2020.07.003.

Kruse, Clemens Scott, R. S. Frederick, T. Jacobson, and D. Monticone. 2017. "Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends." Technology and Health Care 25 (1): 1–10.

Li, Jinhong, et al. 2023. "Assessing the Impact of Health Information Exchange on Hospital Data Breach Risk." International Journal of Medical Informatics 177: 105149. https://doi.org/10.1016/j.ijmedinf.2023.105149.

Oh, Se-Ra, Young-Duk Seo, Euijong Lee, and Young-Gab Kim. 2021. "A Comprehensive Survey on Security and Privacy for Electronic Health Data." International Journal of Environmental Research and Public Health 18 (18): 9668. https://doi.org/10.3390/ijerph18189668.

Piasecki, Jan, Ewa Walkiewicz-Żarek, Justyna Figas-Skrzypulec, Anna Kordecka, and Vilius Dranseika. 2021. "Ethical Issues in Biomedical Research Using Electronic Health Records: A Systematic Review." Medicine, Health Care and Philosophy 24: 633–658.

Snyder, et al. 2022. "Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis." Journal of Medical Internet Research.

World Health Organization. 2021. Ethics and Governance of Artificial Intelligence for Health: WHO Guidance. Geneva: World Health Organization.

***

Acknowledgment
None

Funding Information
None

Conflicting Interest Statement
The authors state that there is no conflict of interest in the publication of this article.

Publishing Ethical and Originality Statement
All authors declared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.

Generative AI Statement
N/A