



Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

TWENTIETH CONGRESS
First Regular Session

House Bill No. **2463**



Introduced by **Representative GIRLIE E. VELOSO**

EXPLANATORY NOTE

In an increasingly digital world, the right to health signifies the right to access, protect, and benefit from one's own health information. International models of a unified digital health infrastructure as in New Zealand, Estonia, and Finland improved the health system in terms of efficiency, equity, and clinical safety. It represents a strategic convergence of the principles of patient empowerment, universal health access, and state accountability. As such, health data under a whole-of-government and whole-of-society approach to health information system becomes a right, a resource, and a tool of dignity for all. It calls for a shift in paradigm from treating health records as static documents to utilizing it as dynamic assets that empower the system and the people.

In the Philippines, the current state of digital health systems remains provider-centric, highly fragmented, and inaccessible to the patient. While certain programs and hospitals systems are digitized, these initiatives operate in silos and lack a common denominator for integration. Patients are repeatedly required to manually fill out numerous forms, carry printed test results, and recount by memory their medical history, leading to gaps in care, missed diagnoses, and out-of-pocket expenses that could have been avoided. The absence of a legal framework governing the structure, access, ownership, and use of health data leaves both patients and providers vulnerable to inefficiency, medical errors, and privacy violations

This Bill seeks to institutionalize a rights-based, policy-coherent, patient-centered, interoperable, and secure digital health infrastructure that consolidates an individual's medical journey across time, institutions, and geographies. By linking each record to a National Health Identity through the creation of a Unified Health Record System (UHRS), this Bill seeks to provide continuity of care, reduce administrative fragmentation, and eliminate costly redundancies that burden both patients and providers. It transforms data into a backbone of service delivery, unlocking long-term efficiencies while strengthening the individual's agency over their own care decisions. Furthermore,

in the context of our archipelagic population, rising non-communicable diseases, growing mobile and overseas populations, and increasingly digital public services, this Bill uses technology as a bridge of care and a tool for informed decision-making.

The UHRS is a cornerstone reform that entails both immediate health service improvements and lasting institutional transformation. This centralized, patient-accessible digital health records can significantly improve health outcomes, increase trust in public services, and reduce long-term healthcare costs through continuity and coordinated care. Clinically, the system enables timely access to accurate, longitudinal data, leading to more confident diagnoses, reduced medical errors, and improved medical decision-making. Hence, real-time, life-saving decisions are better made especially during emergencies. It also minimizes repetitive paperwork, streamlines referrals, and enhances inter-professional coordination. In a patient's perspective, the UHRS turn patients from passive recipients to active partners of their health care journey. It lowers the emotional and financial cost of fragmented care by reducing the need to repeat tests, explain medical histories, or manually transport printed records. While this Bill requires upfront investment in systems, training, and implementation, it offers generational and exponential returns in the form of cost savings, healthier populations, and digital governance maturity by reducing long-term administrative overhead, improving service delivery metrics, and increasing public satisfaction in health institutions.

By institutionalizing the UHRS, the State affirms its commitment to people-first health governance, universal health care, and digital transformation. It serves as a resilient digital backbone, where the burden of recall, repetition, and reprinting no longer falls on the sick and the poor. This Bill lays the groundwork for cross-agency and inter-professional data collaboration while preserving privacy and consent, ultimately supporting a more connected, inclusive, and humane healthcare system.

In view of the foregoing, support for the enactment of this measure is earnestly sought.


REP. GIRLIE E. VELOSO
Malasakit@Bayanihan Partylist



Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

TWENTIETH CONGRESS
First Regular Session

House Bill No. **2463**

Introduced by **Representative GIRLIE E. VELOSO**

**AN ACT ESTABLISHING THE UNIFIED HEALTH RECORD SYSTEM AND THE
NATIONAL HEALTH IDENTITY FOR FILIPINOS, AND INSTITUTIONALIZING A
PATIENT-CENTERED, INTEROPERABLE ELECTRONIC HEALTH
INFRASTRUCTURE**

Be it enacted by the Senate and House of Representatives of the Philippines in Congress assembled:

1 **SECTION 1. Short Title.** — This Act shall be known as the “Unified Health Record
2 System Act”.

3 **SECTION 2. Declaration of Policy.** — It is the policy of the state to promote and protect
4 the right to health of all Filipinos through an equitable, efficient, responsive, and people-centered
5 healthcare system. To honor this commitment, the State shall establish a Unified Health Record
6 System anchored on a National Health Identity, ensuring improved health outcomes, continuity of
7 care, and rational use of public resource while upholding the rights to privacy, informed consent, and
8 access to health data governance and service delivery.

9 **SECTION 3. Definition of Terms.** — As used in this Act:

- 10 (a) Electronic Health Record refers to the longitudinal, digital record of a person’s health
11 history, including diagnoses, prescriptions, procedures, laboratory results, immunizations,
12 allergies, and other relevant information necessary for the delivery of health care.
13 (b) Unified Health Record System (UHRS) refers to the nationwide digital infrastructure that
14 securely integrates and enables access to electronic health records across all accredited
15 health facilities, anchored on a unique health identity.

- (c) National Health Identity (NHI) refers to the unique and permanent identifier assigned to each Filipino or legal resident for health purposes, and used across all healthcare interactions.
- (d) Health Facility refers to any institution, whether public or private, that delivers health services, including hospitals, clinics, rural health units, barangay health stations, laboratories, virtual care entities, and other health service providers.
- (e) Interoperability refers to the ability of health information systems, software, and applications to communicate, exchange, and use health data effectively and securely.
- (f) Health Record Entry refers to any digital record encoded or uploaded into the UHRS that corresponds to a distinct health service rendered to a patient, including but not limited to consultations, diagnostics, procedures, prescriptions, certificates, referrals, and admissions.

SECTION 4. Establishment of the Unified Health Record System (UHRS). — The Department of Health (DOH,) in coordination with the Department of Information and Communications Technology (DICT), shall establish and maintain the Unified Health Record System (UHRS) as the official and centralized digital infrastructure for managing electronic health records of all citizens and residents of the Philippines.

The DOH and the DICT shall be supported by:

- (a) The Philippines Health Insurance Corporation (PhilHealth) for financial claims, benefits, and fraud prevention mechanisms;
- (b) The National Privacy Commission (NPC) for data protection and compliance, and overseeing breach management;
- (c) The Department of the Interior and Local Government (DILG) for the coordination with local government health units; and
- (d) The Philippine Statistics Authority (PSA) for the integration of Philippine Identification System (PhilSys) to ensure identity authentication and portability.

SECTION 5. UHRS Functions and Standards. —The UHRS shall:

- (a) Assign an NHI to each patient based on their PhilSys Number, for consistent identification across all health services;
- (b) Restrict the creation, updating, and modification of electronic health records to authorized personnel from accredited health facilities and licensed health professionals, ensuring data integrity and accountability;
- (c) Enable real-time and role-based access to electronic health records across all levels of care and accredited health facilities;
- (d) Allow patients and their authorized representatives to view their electronic health records through a secure, government-managed or government-accredited portal or mobile application, subject to authentication and privacy safeguards;

- (e) Ensure the provision and development of the necessary digital infrastructure, including reliable connectivity, secure physical or cloud-based servers or data storage, system redundancy, regular backups, cybersecurity protocols, and interoperable software platforms;
- (f) Support continuity of care across in-person and virtual care consultations, emergency attention, medical treatment, diagnostics referrals, and public health surveillance;
- (g) Ensure interoperability with systems of the DOH, PhilHealth, local government units (LGUs), and other relevant public and private entities; and
- (h) Implement audit trails, access logs, and multi-factor authentication to prevent unauthorized access or tampering, in compliance with national data privacy and cybersecurity standards.

SECTION 6. Coverage and Compliance. — This UHRS shall apply to:

- (a) All public health facilities under the DOH, LGUs, and government-owned or controlled health institutions, which shall fully integrate into the system within three (3) years from the effectivity of this Act;
- (b) All private hospitals, clinics, diagnostic centers, and other health service providers, which shall integrate into the system within five (5) years, subject to phased accreditation and support mechanisms;
- (c) All digital health platforms and software vendors that seek interoperability with public systems shall comply with standards prescribed by the DOH and the DICT;

SECTION 7. Non-Compliance and Sanctions. — Failure to meet with the prescribed timeline and standards for UHRS integration shall subject the non-compliant health facility or provider to administrative sanctions appropriate to their classification and the nature of the violation, including but not limited to:

- (a) Suspension or denial of DOH or PhilHealth accreditation for private providers;
- (b) Withholding of certain budgetary releases or health grants for public health facilities; and
- (c) Disqualification from participating in national health programs until compliance is achieved.

The Implementing Rules and Regulations (IRR) shall detail the levels of non-compliance and the corresponding sanctions, ensuring that enforcement mechanisms are responsive, equitable, and proportional to the degree of violation.

SECTION 8. Accreditation and Enrollment of Private Health Entities. — To ensure full and equitable participation in the UHRS, all private hospitals, clinics, diagnostic centers, and other health service providers shall undergo enrollment and accreditation, which shall be based on compliance with UHRS technical, security, and data standards, including:

- (a) Use of government-accredited UHRS-compliant systems;
- (b) Secure infrastructure for data encoding, transmission, and storage, in line with privacy and cybersecurity laws;
- (c) Designation of qualified personnel responsible for electronic health record management and compliance; and
- (d) Demonstrated capacity to uphold patient rights, data integrity, and confidentiality standards.

SECTION 9. Support Mechanisms. — To promote inclusive and sustainable integration, the DOH and the DICT shall implement support mechanisms such as:

- (a) Technical assistance and training for digital on-boarding;
- (b) Access to government-developed or government-accredited UHRS-compliant software;
- (c) Financial or logistical aid, especially for small or rural private providers, subject to availability of funds; and
- (d) Transitional arrangements to enable compliance within the prescribed timeline.

SECTION 10. Data Protection, Access Controls, and Privacy Safeguards. — The UHRS shall be governed by the principles of privacy, security, transparency, accountability, and data minimization. All personal and sensitive health data processed under this Act shall be protected in accordance with applicable privacy and data protection laws, regulations, and issuances. Data collected through the UHRS shall be used solely for lawful health care delivery, public health surveillance, health systems management, or policy development. No part of a patient's health record may be accessed, shared, or used for purposes beyond the scope of this Act, unless with the patient's explicit consent or as otherwise provided by law. The DOH, in coordination with the DICT and NPC, shall ensure full compliance with privacy standards and cybersecurity protocols in the design, implementation, and ongoing operation of the UHRS.

SECTION 11. Documentation of Health Services. — All health record entries shall correspond to a legitimate health service rendered by an accredited health facility or professional.

- (a) All material health services rendered under any accredited facility shall be duly recorded and retained in the UHRS as part of the patient's official electronic health record.
- (b) All health record entries shall adopt the standard documents or formats customarily issued to patients based on the nature of the service, including but not limited to:
 - 1. Medical certificates for employment, education, travel, legal, insurance, or administrative purposes;
 - 2. Prescriptions or clinical notes for check-ups or consultations;
 - 3. Diagnostic results for laboratory or imaging services;
 - 4. Discharge summaries for inpatient admissions or surgical procedures; and
 - 5. Referrals, administrative documents, or PhilHealth claims for other supporting services.

- (c) Each entry must include sufficient identifying metadata, such as the date and time of service, the facility where it was rendered, and the responsible health professional, in accordance with technical standards to be prescribed in the IRR.
- (d) The level of detail to be included may be abstracted, limited, or subject to restricted access based on patient preference, clinical appropriateness, or applicable data protection regulations, as further defined in the IRR.
- (e) Once health data has been duly encoded into the UHRS, patients shall not be required to repeatedly fill out manual health forms, reprint previously submitted records, or physically carry documents such as diagnostic results, prescriptions, or medical histories when accessing care at another accredited facility, except in cases of verified system unavailability. All participating health providers shall retrieve relevant data directly through the system, in accordance with their authorized access privileges and the patient's consent.

SECTION 12. Access Logging and Auditability. — All access to the UHRS, including the viewing, submission, editing, exporting, or transmission of health records, shall be automatically logged by the system. Each log shall record the identity of the user, the affiliated facility, the time and date of access, and the nature of the interaction. These logs shall be securely retained in accordance with data governance protocols, and shall be made available for audit, investigation, or patient review under procedures to be defined in the IRR.

SECTION 13. Role-Based Access and User Registry. — Access to the UHRS shall be limited to verified and approved personnel under accredited health facilities.

- (a) Only accredited health facilities shall be permitted to access the UHRS. Each accredited entity shall declare to the DOH the names, roles, and professional credentials of its personnel authorized to access the system.
- (b) No individual shall be granted access to the UHRS unless their role and credentials have been approved by the DOH or its designated accrediting body. The DOH shall maintain a secure registry of UHRS users, including their declared roles, facility affiliation, and access privileges.
- (c) Health facilities shall update this list regularly and immediately notify the DOH of any change in employment, reassignment, or disqualification. For health professionals with multiple affiliations, system access shall be granted per role and per entity, and shall reflect only the level of access appropriate to each facility's scope and the user's approved responsibilities therein.
- (d) Access to the UHRS shall be limited to what is necessary to perform one's lawful and officially declared functions. Only licensed health professionals may create or modify clinical records, whether directly or through supervised encoding by support personnel.

SECTION 14. Tiered Data Classification and Encryption. — All health record entries in the electronic health record under the UHRS shall be classified and protected according to sensitivity.

(a) Data classification is as follows:

1. General Health Data refers to clinical information routinely generated during the course of care that is not reasonably expected to be sensitive, such as medication history, allergy records, immunization history, and past medical conditions already disclosed to the patient. This data shall be encrypted at the system level and accessible to licensed clinical personnel directly involved in the patient's care.
2. Sensitive Health Data refers to any health information which, by nature or context, may be considered sensitive by the patient or by prevailing ethical or cultural standards, including but not limited to:
 - 2.1. Diagnoses related to mental health, sexually transmitted infections, HIV, reproductive health, or substance use;
 - 2.2. Procedures or findings involving terminal illness, life-threatening conditions, rare diseases, infertility, trauma, abuse, or gender-affirming care;
 - 2.3. Any other medical information that the patient has expressly flagged as sensitive in the system settings.

This data shall be encrypted independently at rest and in transit, with access limited to authorized personnel on a need-to-know basis, and further conditioned on explicit, verifiable patient consent, unless otherwise permitted by law or required in an emergency.

3. Administrative and Operational Data refers to non-clinical information such as referrals, billing and claims, facility usage history, or logistics-related records. This shall be encrypted and accessible only to authorized administrative personnel in accordance with their designated function, and shall not include access to clinical notes or diagnoses unless specifically authorized.
- (b) Attending health professionals shall make reasonable efforts to inform patients of their right to classify certain health information as sensitive. They shall also facilitate the encoding or updating of such designations into the UHRS during or immediately following the relevant health encounter.
- (c) Patients may likewise authorize or unlock access to specific sensitive data at the time of consultation, whether verbally or through a digital confirmation mechanism, for the purpose of ensuring continuity of care. Such real-time consent shall be digitally recorded in the system and may be modified or revoked at any time, subject to proper authentication.
- (d) Sensitive health data shall be stored in encrypted form, segregated from general records, and decrypted only upon verified patient consent or legal exception.
- (e) No user shall access or retrieve information beyond the scope of their authorized role.

SECTION 15. Patient Consent and Control. — Patients shall have access to and control over their own electronic health records.

(a) Patients shall have the right to:

1. Securely view their complete electronic health record through an official UHRS portal or application;
2. Grant or revoke consent for access to specific categories of sensitive data, subject to legally recognized exceptions such as medical emergencies or mandatory reporting;
3. Designate representatives or next of kin to access their records;
4. Request access to a system-generated audit log of interactions, subject to reasonable procedures and safeguards to be defined in the IRR.

(b) Consent to access or disclose sensitive health data shall be informed, voluntary, and revocable at any time, without prejudice to ongoing care. No person shall be compelled to unlock or disclose protected data beyond what is medically or legally required.

SECTION 16. Contextual and Emergency Access. — The UHRS shall allow conditional access for handling role-specific, contextual, and emergency situations.

(a) Default Data Filtering. The UHRS shall present to each user only the subset of information relevant to their role and the specific reason for system access, such as a diagnosis, referral, or lab request. Broader access to historical or unrelated data shall require additional justification or patient consent, except in medical emergencies.

(b) Emergency Override Protocols. In life-threatening situations or public health emergencies, authorized providers may override access restrictions subject to system-logged justification and post-event review.

SECTION 17. Prohibited Acts. — The following are prohibited under this Act and shall be subject to administrative, civil, or criminal liability:

- (a) Unauthorized access, use, alteration, disclosure, or destruction of UHRS data;
- (b) Forcing or coercing any person to disclose or unlock protected health data;
- (c) Accessing or decrypting sensitive data without verified consent or lawful authority;
- (d) Falsifying, deleting, or modifying any electronic health record for unlawful purposes;
- (e) Allowing access by unaccredited individuals or facilities;
- (f) Using UHRS data for discriminatory, defamatory, or unethical purposes;
- (g) Encoding false, misleading, or unreasonably omitted information into the UHRS;
- (h) Refusing to correct verified erroneous data;
- (i) Compromising UHRS security or interfering with its operations;
- (j) Unauthorized or unjustified use of emergency override or contextual access functions, or failure to submit required justification in accordance with system protocols;

- 1 (k) Failure to update access credentials or employment status of personnel with UHRS
2 privileges;
3 (l) Obstructing a patient's lawful access to their health records or audit logs; and
4 (m) Unauthorized duplication, export, or external transmission of UHRS data outside
5 approved channels.

6 Violations shall be classified by severity in the IRR, which shall prescribe corresponding
7 penalties including suspension of access, revocation of accreditation, civil damages, and prosecution
8 under relevant laws.

9 **SECTION 18. Implementing Rules and Regulations.** -- Within ninety (90) days from the
10 effectivity of this Act, the DOH shall, in consultation with the DICT, the NPC, PhilHealth, and
11 other concerned government agencies and stakeholders, promulgate the necessary rules and
12 regulations for the effective implementation of this Act.

13 **SECTION 19. Appropriations.** — The amount necessary for the initial implementation of
14 this Act shall be charged against the current appropriations of the DOH, the DICT, and other
15 concerned government agencies; and against the Special Health Fund and other applicable local
16 sources of the LGUs. Thereafter, the funds necessary for the continued implementation of this Act
17 shall be included in the annual General Appropriations Act.

18 The DOH, in coordination with the DICT and the Department of Budget and Management
19 (DBM), shall prepare a multi-year implementation and investment plan to cover the costs of
20 infrastructure, system development, accreditation support, training, maintenance, and cybersecurity,
21 with priority given to under-resourced health facilities and LGUs.

22 **SECTION 20. Repealing Clause.** — All laws, decrees, executive orders, rules and
23 regulations, or parts thereof inconsistent with the provisions of this Act are hereby repealed or
24 modified accordingly.

25 **SECTION 21. Separability Clause.** — If, for any reason, any section of this Act shall be
26 deemed unconstitutional or invalid, the other sections or provisions shall not be affected and shall
27 remain in force and in effect.

28 **SECTION 22. Effectivity Clause.** — This Act shall take effect after fifteen (15) days from
29 its publication in the Official Gazette or in at least two (2) national newspapers of general
30 circulation, whichever comes earlier.

31 Approved.