

Title 41 - Health Information and Patient Privacy Act 2026 (HIPPP)

Preamble:

Recognising that confidentiality and trust are essential to effective healthcare; affirming the rights to privacy, dignity, equality, access to personal information and safe treatment; and acknowledging that health information requires safeguards in addition to the general framework of the Data Protection Act 2026 and the duties of the Linkslandic Health Service Act 2026, this Act establishes patient-centred rules for the handling of health information. This Act works in conjunction with and is read alongside the Data Protection Act 2026, the Linkslandic Health Service Act 2026, the Child Safety and Protection Act 2025, the Senior Dignity and Welfare Act 2025, the Unity and Equality Act 2025, the Public Administration Efficiency Act 2025, the Online Safety and Digital Services Act 2025, the National Secrets Protection and Official Secrecy Act 2025 and the Public Health Preparedness Act 2025.

Article 1: Purpose and Scope

Section 1A — Purpose

(a) The purpose of this Act is to protect the confidentiality, integrity, availability and appropriate use of health information.

(b) This Act applies to the Linkslandic Health Service and to every public or private provider that creates, receives, stores or uses a health record in Links Land.

Section 1B — Interpretation

(a) Health record means recorded information relating to a person's physical or mental health, treatment, diagnosis, care, genetic information or health-related identity information.

(b) Health provider includes a clinician, contractor, facility, insurer where lawfully holding a health record, and an information-technology service acting for a provider.

(c) Nothing in this Act removes a protection or duty under another Act. Where duties overlap, the provider shall comply with the stronger applicable protection and the minimum necessary disclosure rule.

Article 2: Confidentiality and Lawful Use

Section 2A — Confidentiality

(a) A health provider shall keep a health record confidential and shall use or disclose it only for treatment, care coordination, payment, administration, quality and safety, public-health protection, safeguarding, research, planning, a legal obligation, a judicial order, or another purpose authorised by law.

(b) A disclosure shall be limited to the information reasonably necessary for its purpose.

Section 2B — Sensitive Information

(a) Sexual orientation, gender identity, intersex status, legal gender information and comparable sensitive identity information shall be treated as restricted fields.

(b) A restricted field shall be recorded, displayed or disclosed only where clinically necessary, authorised by the patient, required by law, necessary for safeguarding or statutory notification, necessary to prevent imminent serious harm, or required by a judicial order.

(c) Restricted fields shall not appear on a default user interface where their display is not necessary for the user's role.

Section 2C — Young People

(a) A young person may consent to treatment and may access that person's own health record where the clinician reasonably determines that the young person understands the nature, purpose, consequences and confidentiality of the decision.

(b) Where a young person lacks that understanding, the provider shall apply the lawful parental or representative-access rules and shall protect the young person's welfare.

(c) A provider shall assess competence, coercion and risk of abuse in accordance with the Child Safety and Protection Act 2025. This section does not prevent a report or action required by law.

Article 3: Patient Rights

Section 3A — Access and Audit

(a) A patient has the right to obtain a copy of the patient's health record and an audit log identifying each person or system that accessed it, the date of access and the recorded purpose.

(b) A provider shall respond to an access or audit-log request within 14 business days, subject to lawful identity verification and a narrowly tailored restriction necessary to prevent serious harm or protect another person's confidential information.

Section 3B — Correction

(a) A patient may request correction of inaccurate or incomplete information.

(b) A provider shall correct the record or attach a clearly visible statement of the patient's requested correction within 14 business days, retaining the original entry where necessary for clinical integrity and auditability.

Section 3C — Research and Planning

(a) A patient may opt out of the use of identifiable health information for non-essential research or service-planning purposes, subject to a lawful overriding public-health requirement.

(b) Where information is used without an opt-out, it shall be anonymised or appropriately de-identified wherever the purpose can reasonably be achieved without identifying the patient.

Article 4: Security and Breach Response

Section 4A — Security Controls

(a) A health provider shall use encryption appropriate to the risk, role-based access controls, authentication, audit logging, access review and secure disposal procedures.

(b) A provider shall maintain a breach-response process and shall train personnel in confidentiality, restricted fields, emergency access and safeguarding duties.

Section 4B — Breach Notification

(a) A provider shall report a qualifying breach in accordance with the 72-hour reporting requirement in the Data Protection Act 2026.

(b) Every patient affected by a qualifying breach shall be notified without undue delay, regardless of whether the provider considers the risk threshold under another Act to be high. The notice shall describe the nature of the breach, likely consequences and protective steps.

Section 4C — Emergency Access

(a) A provider may use a break-glass procedure where access is reasonably necessary to protect a patient's vital interests or provide urgent care and ordinary access is unavailable or unsafe.

(b) The user shall record the reason, the information accessed and the time of access. An authorised reviewer shall examine the access within seven days.

Article 5: Disclosure to Public Authorities and Special Records

Section 5A — Lawful Disclosure

(a) Nothing in this Act prevents a report required by the Child Safety and Protection Act 2025, the Senior Dignity and Welfare Act 2025, the Public Health Preparedness Act 2025 or another enactment.

(b) Police access to a health record requires a judicial order except where the Data Protection Act 2026 permits emergency access to prevent a real and immediate threat to life. An emergency access decision shall be submitted for judicial review as soon as practicable.

Section 5B — Classified Information

(a) A person handling a health record that contains classified information shall comply with the applicable clearance, handling and disclosure requirements of the National Secrets Protection and Official Secrecy Act 2025.

(b) Classification shall not by itself remove a patient's right to obtain the patient's own record, but access may be arranged through a lawful secure process and subject to a specific lawful restriction.

Article 6: Offences and Enforcement

Section 6A — Inappropriate Access

(a) A person who, having legitimate technical access to a health-record system, intentionally accesses or uses a health record without a lawful purpose commits an offence.

(b) The offence is a Low Offence punishable by imprisonment for up to three years or a fine not exceeding 50,000 Links Landic Dimes, or both, subject to the Criminal Proceedings Act 2025.

(c) This section does not apply to good-faith treatment, safeguarding, audit, security, emergency, legal or oversight activity carried out within the person's lawful role.

Section 6B — Provider Duties

(a) A provider that persistently or recklessly fails to maintain the safeguards required by this Act may be subject to compliance directions, remedial orders and any applicable penalties under the Data Protection Act 2026 or another enactment.

(b) Enforcement shall be proportionate to the provider's size, resources, culpability, duration of non-compliance and harm caused.

Article 7: Records and Retention

Section 7A — Retention

(a) A provider shall retain an adult's health record for at least eight years after the person's last treatment, unless a longer period is required by law, clinical necessity, litigation hold or an approved records schedule.

(b) A provider shall retain a child's health record until the child's twenty-fifth birthday or for eight years after the last treatment, whichever is later, unless a longer period is required by law or clinical necessity.

(c) After the retention period, information shall be securely destroyed or irreversibly anonymised, subject to lawful preservation requirements.

Article C: Constitutional Compliance

Section C1 — Rights and Proportionality

(a) This Act shall be interpreted consistently with constitutional rights to dignity, privacy, equality, healthcare, due process and freedom from arbitrary state interference.

(b) Any restriction on access, disclosure or correction shall be lawful, necessary, proportionate and no broader than required to protect a patient, another person's rights, public safety or a compelling public-health interest.

Section C2 — Legal Alignment

(a) This Act works in conjunction with and is read alongside the Data Protection Act 2026 and the Linksländic Health Service Act 2026. It does not remove any protection, duty, remedy or enforcement power under those Acts or any other enactment.

(b) The constitutional courts retain their jurisdiction to review the legality and proportionality of action taken under this Act.