Humanetix Privacy Policy

Humanetix offers a unique safety critical workflow engine (SWE) for hospitals, aged care facilities and other clinics. Humanetix SWE provides an Electronic Health Record (eHR), decision support and quality assurance at all stages of care to deliver better patient outcomes, while reducing healthcare costs.

We are committed to supporting our customers in protecting the privacy of patient information and to handling personal information in accordance with the Privacy Act 1988 (Commonwealth), the Privacy Amendment (Enhancing Privacy Protection) Act 2012, the Australian Privacy Principles and relevant State and Territory privacy legislation.

Humanetix customers are hospitals, aged care facilities other healthcare providers or an individual clinician. These customers, or in some cases, individual clinicians working in those clinics, make care plans and records using Humanetix and are the owners of these medical plans and records to the extent that they are their business record and property. However, the patient is the ultimate owner of the information in the record. Patient privacy requires that the patient information is kept confidential, secure and that the data retains integrity.

This policy describes Humanetix approach to helping its customers maintain patient privacy. The policy is an integral part of Humanetix Quality Management System (ISO9001 certified) and relevant staff are trained to understand its rationale and to implement it in company operations.

Confidentiality

Humanetix software enables its customers to record and store patient information. Humanetix recognises that patient information should be released to others only with the patient's permission or as allowed by law.

Responsibility for obtaining patient permission to release data, and decisions on to whom this information is released, are the responsibility of the customer that has licensed Humanetix software. Humanetix does not deal directly with patients and refers any queries from patients about data held in the Humanetix system to the customer to manage.

Humanetix staff only access or copy individual patient information when needed to diagnose issues reported by customers or to monitor system performance and when authorised by the customer to do so. When copied, all data is de-identified according to company-approved procedures to ensure no identifiable patient data leaves the production data environment.

Only individuals authorised by the hospital clinic, aged care facility, other clinic or the clinician become registered users within Humanetix. The nominated customer representative identifies the various staff roles within the clinic or facility and determines what information is needed by each role.

The customer's system administrator, nominated by the customer representative, creates user accounts within the customer's own identity store. Management of these user accounts and related authentication credentials is the responsibility of the customer.

Security

In addition to supporting its customers to maintain confidentiality through appropriate permissions and user access, Humanetix also supports its customers' security policies and procedures to protect patient information against unauthorised external access.

Humanetix is ISO 9001 certified through its entire development process.

Humanetix implements the following measures to ensure data security:

- Humanetix applications are deployed to a secure cloud environment located within Australia;
- Humanetix applications are deployed within a dedicated environment for each individual customer; that is, Humanetix operates different tenancies within the same environment;
- Humanetix applications use secure-HTTP for all communication between client applications and back-end; that is, all data is encrypted while in transit over the public internet;
- Access to Humanetix applications can be restricted to particular IP addresses;
- User identification is separated within the application; all clinical data is stored detached from the user identity and only re-identified in the client application;
- Resident/Patient identification is equally separated within the application; all clinical data is stored detached from the resident/patient identity and only re-identified in the client application;
- Humanetix offers the facilitation of all client application data access via a VPN to further enhance data access security.

Humanetix co-operates with the customer on the physical security of and access to client hardware running Humanetix applications. Each party's responsibilities are specified in a in Service Level Agreement with the customer. Generally, the customer's responsibility includes:

- Controlling the use of devices to transmit data is the responsibility of the customer;
- Setting and enforcing policies for strong authentication factors;
- Educating all users as the above;
- Ensuring the physical security of all client devices, for example—but not exclusively—against theft and loss;
- Securing the in-facility network, wired or wireless;
- Ensuring effective malware detection and removal measures are in place for all client devices;
- Ensuring effective detection measures are in place for the leakage of clinical data outside the facility.

Humanetix also co-operates with the customer in the implementation of a data disposal plan and in the removal of data from reusable hardware.

Should an unauthorized user gain access to clinical information contained in Humanetix, Humanetix will assist the customer, to the extent practical, to identify the extent of the unauthorised access and to enable the Customer to notify affected patients if that is required.

Data Integrity

Humanetix recognises that data used in clinical decision-making must be accurate. The responsibility for taking measurements, and entering data accurately, rests with the customer's staff. Once entered into a Humanetix SWE, all data is time, date and user identity stamped. Once saved into a Humanetix SWE, data can be changed by an authorised user. In that event, the previous record is retained and the date, time and identity of the user making the change is recorded.

Humanetix SWE may alert a clinician that an abnormal observation has been entered. This will be according to rules and guidelines provided officially to Humanetix by the customer and responsibility for the integrity of the rules and guidelines lie exclusively with the customer.