

Documento de FOLLOWHEALTH S.L

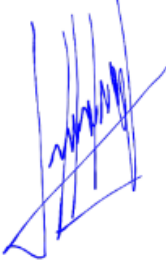

Information Security Policy

FOLLOWHEALTH S.L

05/04/2024

Contacto: legal@humanitcare.com

<https://humanitcare.com/>

	Creado por	Revisado y aprobado por
Nombre	Eduardo Alf	Nuria Pastor Hernández
Función	Responsable SGSI	Directora General
Fecha	24/11/2020	05/04/2024
Categoría	Política	
Firma		

Versión	Fecha	Control de cambios	Responsable aprobación
1.0	24/11/2020	Documento inicial	Nuria Pastor Hernández
2.0	05/04/2024	Documento actualizado	Nuria Pastor Hernández

Policy

FollowHealth's Security Policy reflects the principles and objectives regarding information security, which results allow our company to achieve its purpose of the implementation of the ISO 27001, according to the scope of the Management System that is "The information systems that support the design, development and maintenance of software for telemedicine services and telemonitorization, according to the current applicability statement."

By developing, communicating and maintaining this policy, FollowHealth's Management shows its commitment to protect the confidentiality of the information, guarantee its integrity in all the treatment processes, as well as the availability of the information systems involved in these treatments.

For this, FollowHealth's Management has defined and implemented an Information Security Management System -ISMS- that allows the company to comply with:

- Information security through Human Resources Management, before, during and at the end of employment.
- Proper asset management that implies the classification of information and the correct manipulation of assets, and the establishment of a robust logical access control to its systems and applications, managing the permissions and privileges of the users.
- Facilities and physical environment protection, through the design of safe work areas and equipment security.
- Ensuring security in operations by protecting against malicious software, performing backups, establishing logs and monitoring them.
- Control of the software in operation.
- The management of technical vulnerabilities.
- Communications security, protecting networks and information exchange.
- The security assurance through the acquisition and maintenance of information systems, limiting and managing change.
- Carrying out a secure software development, separating environments, and carrying out functional and acceptance tests.
- The control of relationships with suppliers, demanding compliance with security measures contractually, and monitoring acceptable levels in their services.
- Managing security incidents efficiency, establishing the appropriate channels for their notification, response and timely learning.
- Carrying out a business continuity plan that protects the availability of services during a disaster.
- Compliance with applicable regulations, especially intellectual property and protection of personal data.
- Periodic reviews and continuous improvement of our ISMS to guarantee compliance and effectiveness of these requirements.

Signed: *Management*