Shanghai United Imaging Healthcare Co., Ltd.

Shanghai, China
2258 Chengbei Rd., Jiading District, Shanghai, 201807.

Email | info.global@united-imaging.com
Business Consultation | +86（21）- 67076666
After-sales Service | 4006 - 866 - 088

ABOUT UIH

At United Imaging, we develop and produce advanced medical products, digital healthcare solutions, and intelligent solutions that cover the entire process of imaging diagnosis and treatment. Founded in 2011 with global headquarters in Shanghai, our company has subsidiaries and R&D centers across China, the United States, and other parts of the world. With a cutting-edge digital portfolio and a mission of broader access to healthcare for all, we help drive industry progress and bold change.

To learn more, visit https://www.united-imaging.com

UNITED IMAGING

Cybersecurity Statement

Version | 91000116-CSD-SCN-02, June, 2025

External Environmental Changes

In the era of digital economy, data elements have become the core driving force for the development of new technologies in various industries. With the rapid development and deep integration of technologies such as big data, cloud computing, and Internet of Medical Things (IoMT), the healthcare industry is experiencing an unprecedented wave of informatization reform. New trends such as healthcare devices, integrated diagnosis and treatment, and smart healthcare have emerged. The trend of digitalization, intelligence, and interconnection in the healthcare industry is irreversible, but at the same time, the industry and enterprises are also facing more severe network and data security risks and challenges.

In response to the frequent data and cybersecurity threats, the global regulatory system has been accelerated and improved. Many countries or regions have promulgated legislation to comprehensively implement data security protection measures. For example, China's Data Security Law of the People's Republic of China, Cybersecurity Law of the People's Republic of China, the United States' Health Insurance Portability and Accountability Act (HIPAA), California Consumer Privacy Act (CCPA), and the European Union's General Data Protection Regulation (GDPR), etc.

Medical regulatory agencies in various countries have also successively issued industry standards or guidelines on the cybersecurity of medical devices. China's NMPA Guidelines for Cybersecurity Registration Review of Medical Devices (2022 revised edition) clearly requires enterprises to establish a deep cybersecurity defense system; the U.S. FDA issued Cybersecurity in Medical Devices: Quality System Considerations and Premarket Submissions (2023 final edition), etc., which further emphasize the cybersecurity of medical devices.

Our Actions

UIH pays attention to changes in the external environment and attaches great importance to cybersecurity and compliance. The security and compliance of products and services have always been one of the key development strategies of UIH.

UIH pays attention to the compliance requirements of various countries and regions, actively responds to the security and compliance needs of all stakeholders and the industry, and protects customer interests. To this end, UIH established the Information Security Department in 2012, established the Information Security Supervision and Management Committee in 2016, built an enterprise security internal control system based on risk management and industry best practices in 2017, and successively passed security compliance certifications and tests with broad recognition in different countries, regions, and even internationally from 2017 to 2024

Timeline

2011

UIH Medical was established

2012

UIH Information Security Department was established

2013

The first generation of products was launched

2014

U.S.: Cybersecurity Management of Medical Devices - Premarket Submissions

2016

U.S.: Postmarket Management of Medical Device Cybersecurity

2017

First certification of ISO/IEC 27001:2013

2018

Issued the Product Network Security Procedures

2019

NIST CSF 1.0 Compliance Assessment: Good

2021

Introduced the concept of secure software development life cycle management

CCRC Level 2 certification

2022

ISO/IEC 20000:2018 certification

CCID Assessment: Level 1 Five Stars

2024

IISO/IEC 27001:2022 upgrade certification

ITSS Level 3 certification

NIST CSF 2.0 Compliance Assessment: Excellent

"Gongfu Liwang" Network Protection Action: zero points lost and won the title of excellent blue team

Security Certification and Compliance with Best Practices

UIH has established and operates an Information Security Management System (ISMS) and a Privacy Protection Management System (PIMS) in compliance with ISO/IEC international standards. Based on the ISO/IEC 27000:2022 series, it integrates the Enterprise Cybersecurity Framework (CSF 2.0) issued by the National Institute of Standards and Technology (NIST) into the system, dynamically identifies the information security and privacy regulatory requirements and best security practices of various countries and regions, and continues to improve following the PDCA methodology. This ensures that it can provide customers with secure and compliant products and services, meeting the security and compliance needs of customers in different regions and countries.

ISO 27000 Series

ISO/IEC 27001
Information Security Management System

A set of widely recognized security management system standards in the industry, has always been considered the most authoritative and strict Information Security Management System (ISMS) certification standard in the world, and is widely accepted globally. UIH's certification under this standard means that we have benchmarked international standards in the field of information security management, have sufficient information security risk identification and control capabilities, and can provide safe and reliable services to global customers.

ISO/IEC 27701
Privacy Information Management System

It is the first Privacy Information Management System (PIMS) standard that truly constructs a complete PDCA operation closed loop. It specifies in detail the requirements for establishing, implementing, maintaining, and continuously improving a privacy information management system, and takes into account the privacy protection measures required for processing Personally Identifiable Information (PII) on the basis of information security protection. UIH is one of the first global medical device manufacturers to obtain this certification, which helps ensure privacy compliance in the process of serving customers.

ISO 27799
Healthcare Security Management System

It is a set of Healthcare Security Management System (ISMH) standards that particularly focus on the challenges faced by the healthcare sector. It focuses on the confidentiality, integrity, and availability of personal health information and ensures that access to such information can be audited and held accountable. This helps prevent errors in medical practice while ensuring the continuity of medical services. UIH is one of the first medical device manufacturers to pay attention to this certification. Obtaining this certification means that we provide you with safe and collaborative products and services by adhering to the framework and principles of ISO 27799, which helps you safely adopt collaborative technologies to provide healthcare services and significantly improve medical outcomes.

ISO/IEC 27017
Cloud Service Information Security Management System

It puts forward recommendations for implementing cloud-specific information security control mechanisms, supplementing the guidance of ISO 27002 and ISO 27001 standards. This standard provides more guidance on the implementation of information security controls for cloud service providers. UIH's certification under this standard means that our cloud service products and services have reached international standards.

ISO/IEC 27018
Public Cloud Privacy Security Management System

It is the first international certification standard focusing on the protection of personal information in public clouds. Based on the ISO 27002 Code of Practice for Information Security Management, it provides implementation guidelines for a security control system applicable to Personally Identifiable Information (PII) in public clouds. UIH's certification under this standard means that we have reached the high standards of industry practice in protecting enterprise data, ensuring the security of users' personal information, and preventing information leakage.

Security Certification and Compliance with Best Practices

NIST Cybersecurity Framework CSF 2.0

It is a set of standards, guidelines, and best practices for managing cybersecurity-related risks issued by the National Institute of Standards and Technology (NIST). NIST CSF refers to globally recognized standards, including parts of NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations. In 2019, a third-party evaluation agency with broad international recognition carried out a comprehensive evaluation of UIH based on NIST CSF 1.0, and the score was good. In 2024, when NIST released the official version of CSF 2.0, UIH was again comprehensively evaluated based on version 2.0, and the score was excellent. This indicates that UIH's products are capable of providing good cybersecurity protection for customers, and UIH's security construction is continuously optimized and developed.

Level 3 Cybersecurity Classified Protection

GB/T 22239—2019 Information Security Technology Basic Requirements for Cybersecurity Classified Protection, referred to as Cybersecurity Classified Protection, is an information security standard issued by the Standardization Administration of the People's Republic of China and a basic system for information security protection in the People's Republic of China. UIH has adopted the protection strategy of Class 3 Equal Protection and passed the evaluation of a professional evaluation agency. This indicates that UIH's products have reached the best industry practice level in terms of the ability to detect and respond to security incidents and the recovery ability when information systems are damaged.

Cryptographic Application Security Assessment

It puts forward more stringent requirements for cryptographic application security on the basis of classified protection. It quantitatively evaluates the security, standardization, and effectiveness of eight aspects, including global cryptographic application technology management, physical environment, network communication, and device computing. UIH's products have carried out cryptographic application security assessments and passed the assessments of professional assessment agencies. This indicates that UIH's products and services are capable of helping you use and manage passwords more standardly, maintain the password security of your network and information systems, and effectively protect network security and data security.

UIH actively follows up on the requirements for product safety and compliance at home and abroad, connects with regulatory agencies at all levels through the safety management and compliance team, and ensures that the provided products and services comply with industry standards. It is also equipped with a special privacy protection team to review the privacy protection design of products, privacy policies, and the collection and use of users' privacy data, ensuring that users' privacy data are properly used and processed and maintaining reasonable transparency to users.

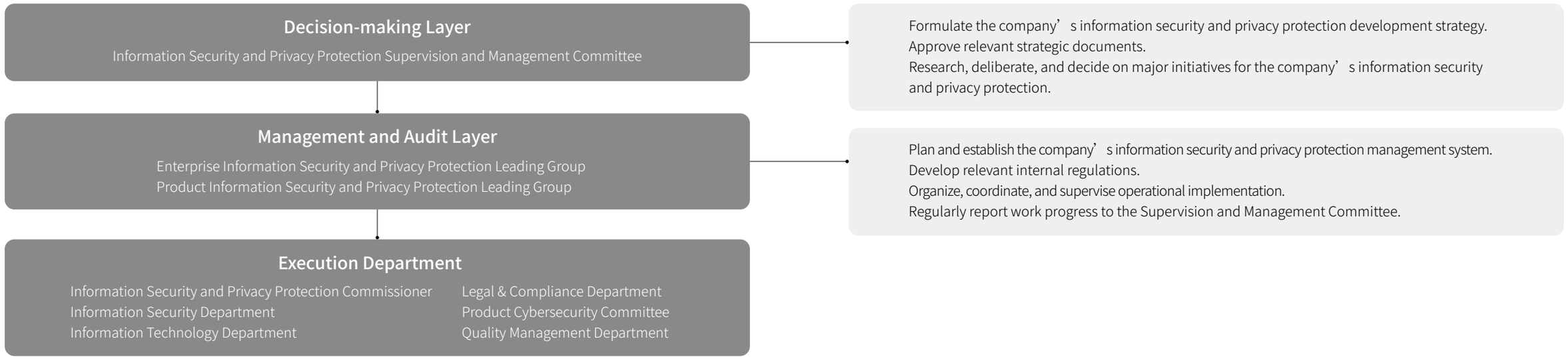
Information Security Governance Organizational Structure

Governance Organizations

Through the systematic construction of information security governance organizations and mechanisms, UIH can provide customers with services in line with international standards and specifications for information security and privacy protection.

UIH has established an Information Security and Privacy Protection Supervision and Management Committee to coordinate and be responsible for the company's information security and privacy protection construction work

UIH Information Security Governance Organizational Structure



Information Security Governance Organizational Structure

UIH Information Security Governance Organizational Structure

Decision-making Layer

The Information Security and Privacy Protection Management Committee, as the decision-making layer, is responsible for formulating the company's information security and privacy protection strategic direction and goals, and studying, deploying, and deliberating on the company's information security and privacy protection work plans and major matters. The committee is composed of senior company executives who are deeply involved in corporate security governance.

Management and Audit Layer

The Enterprise Information Security and Privacy Protection Leading Group and the Product Information Security and Privacy Protection Leading Group together form the management and audit layer. The Enterprise Information Security and Privacy Protection Leading Group and the Product Information Security and Privacy Protection Leading Group are respectively responsible for the security and privacy protection construction in enterprise operations and product research and development. They are relatively independent and work together. The management and audit layer is responsible for implementing the company's security strategy, clarifying the company's operational and product security baselines, participating in the discussion of major company security matters, updating the company's security management system in real-time in combination with changes in the external environment and the expectations of stakeholders, integrating security elements with the company's daily operations and product research and development processes, and promoting their implementation.

Execution Layer

The Information Security Department, Legal Compliance Department, Information Technology Department, Quality Management Department, and information security and privacy protection commissioners of each business department together form the execution layer of security governance. Through planning, execution, monitoring, and improvement, the whole process of enterprise operations and product research and development is safely controlled to ensure that the company's security and privacy protection policies are effectively implemented.security elements with the company's daily operations and product research and development processes, and promoting their implementation.

UIH ensures that the company's information security and privacy protection strategies and goals are implemented and continuously developed and updated through a two-line cycle of top-down promotion and bottom-up feedback.

Information Security Governance Organizational Structure

Personnel Management

In order to standardize employees' information security behaviors during entry, employment, and departure, and reduce information security risks caused by human factors, UIH has established company-wide personnel safety management regulations and processes, and promoted the implementation of personnel safety management requirements through various channels, including but not limited to

Clarify the Division of Responsibilities for Personnel Management

For all key responsibilities of personnel management, clarify the minimum execution units to ensure that security requirements are implemented

Pre-employment Background Investigation

Ensure that personnel backgrounds and experiences meet job and customer requirements

Sign Confidentiality Agreements

Clarify the confidentiality obligations of key positions

Institutional Constraints

Formulate and issue the Personnel Information Security Management Regulations to clarify the company's security requirements at the personnel management level

Access Rights Control

Ensure that personnel rights meet the principle of minimum necessity through approval authorization, rights review and audit, and permission cleanup for job transfer and departure, so as to protect data security

Information Security Governance Organizational Structure

Security Training

In order to raise all employees’ awareness of information security and privacy data protection, UIH

Security Awareness Training

UIH carries out information security awareness training through online and offline lectures every year, covering key contents such as office environment security, password setting security, identifying and preventing phishing emails, protecting trade secrets, and information security during business trips. The training coverage rate for employees reaches 100%

Regular Drills

Regularly carry out phishing email and information security incident drills to enhance employees' information security awareness, improve their vigilance against information security attacks, and promptly discover and report various information security incidents

Normalized Audit

Regularly audit and rectify weak account passwords, deploy and implement a password strength management system, and reduce security risks caused by weak passwords

Information Security Month

Carry out the "Information Security Month" theme publicity and education activities every year, invite experts in the field of network security and privacy data protection to hold special lectures, and enhance employees' enthusiasm to understand information security

Information Security and Privacy Protection Technology Construction

Security Technology System

UIH establishes a Defense-in-depth security technology system to provide multi-layer security protection.

Data Security Protection

- Data integrity and authenticity protection
- Sensitive information anonymization
- Hard disk data encryption
- Data transmission encryption

Application Security Protection

- User authentication and authorization
- User access security protection
- Support for emergency access
- Application whitelist
- Audit log
- Security scanning

Host Security Protection

- Operating system security hardening
- Antivirus software
- Regular virus database updates
- Regular security patch updates
- Trusted authentication
- Password management system

Network Security Protection

- Firewall
- Secure encrypted connection
- Network whitelist
- Network access mechanism
- 7*24 hour monitoring duty
- Situation awareness
- Threat intelligence system

Information Security and Privacy Protection Technology Construction

Information Security Incident Management Process

UIH has established an information security incident monitoring and emergency response mechanism to continuously monitor network security risks related to products and operations and respond to and handle internal and external information security incidents. It analyzes vulnerability warnings and security patches released by the software supply chain and security stakeholders, timely responds to risks and upgrades security protection strategies, and always copes with network security threats together with customers.

Network Attack and Defense Drill

UIH actively participates in various network security drill activities, tests and improves network and data security protection and emergency response capabilities through attack and defense drills, and promotes the construction of the company's network and data security protection system. In 2024, UIH Medical actively participated in the "Gongfu Liwang" network protection action organized by the Shanghai Municipal Economic and Information Technology Commission and the "Panshi Action" security network protection activity held by the Shanghai Communications Administration. Through simulated attack tests, the company's information security risk defense capabilities were improved. During the one-month 7*24-hour security protection period, UIH Medical won the title of excellent blue team awarded by the organizer of the "Gongfu Liwang" with an excellent score of zero points, fully demonstrating UIH Medical's professional strength and solid defense line in the field of information security.

Safety and compliance United Imaging is always by your side

UIH attaches great importance to the network security and privacy protection of customers. We will work with customers to create a network security and privacy security environment by maintaining continuous vigilance and identifying changing network security threats. In the wave of medical digitization, UIH and customers join hands to win the future.