Security Standards

Security Vulnerability and Incident Communications

The following contact details should be used for any notifications of security vulnerabilities and security incidents:

Phone: Security Incident Response (SIR) Hotline at 888-255-2554

Email: SIRG@optum.com

Definitions

UHS	United Healthcare Services, Inc., a Minnesota corporation, together with its affiliates.
UHS Information	means information provided by or on behalf of UHS or processed by Vendor on behalf of UHS, that is one of the following: (i) protected health information (as defined by the Health Insurance Portability and Accountability Act); (ii) non-public personal information (as defined by the Federal Gramm-Leach-Bliley Act); (iii) personal data (as defined by the EU's General Data Protection Regulations); (iv) cardholder data (as defined by the Payment Card Industry Data Security Standard); or (v) other personally identifiable information about individuals including social security numbers. UHSUHS.
UHS Information Systems	UHS's (including its affiliates and other vendors') IT and network systems, including cloud systems and devices.
Vendor	A provider of Vendor Processing services to UHS, or a service provider accessing any UHS Information System, as well as their subcontractors for such services.
Vendor Information Systems	Vendor's (including its subcontractors') IT and network systems, including cloud systems and devices, that are used for Vendor Processing, or can be used directly or indirectly to access either systems used for Vendor Processing or UHS Information Systems
Vendor Processing	Any information creation, collection, storage, or processing performed by vendor or its subcontractors of UHS Information.

Standards

The following minimum standards must be met by vendors storing, transmitting, or processing UHS Information or accessing UHS Information Systems in addition to any security standards in our agreement.

Segregation	Vendor must physically or logically segregate UHS Information from other data processed by Vendor.
Encryption	UHS Information must be encrypted in transit and at rest using industry best practice standards.
End Devices	every end device (e.g., mobile, laptop, or workstation) used to process or store UHS Information, or access UHS Information Systems, must: • be vendor-issued or managed (i.e., not a personal device),

	• have up-to-date malware prevention and detection software, • have a firewall, and • have full disk encryption.
Removable Media	Vendor must maintain controls on End Devices to prevent UHS Information being exported to or stored on removable media (e.g., thumb drives, smart cards, or portable drives), unless pre-approved by UHS.
Multi-Factor Authentication	Vendor shall ensure that access to UHS Information, Vendor Information Systems, and endpoints to UHS Information Systems use multi-factor authentication that includes at least two of the three following factors: something the user knows, something the user has, and something the user is.
Portal Security	Vendor shall implement and maintain the following portal security controls for web and mobile applications that interact with or contain UHS Information: (a) multi-factor authentication; (b) BOT activity monitoring and logging; and (c) risk-based authentication.
Secure Deletion	Any UHS Information to be deleted under our agreement must be securely deleted as follows: • Hard copies must be destroyed by shredding or otherwise so that they cannot be reconstructed. • Electronic copies must be deleted and overwritten so that they cannot be retrieved or reconstructed. • Vendor Information Systems equipment that held UHS Information must be physically destroyed, degaussed or overwritten in accordance with NIST Special Publication 800-88 before being disposed of or used for another purpose.
Training & Personnel	All vendor personnel supporting Vendor Processing must receive training at least annually on industry standard security practices, applicable privacy laws and regulations, and their responsibilities for protecting UHS Information. If a vendor user ceases to be an employee or contractor of vendor or its subcontractor, or otherwise involved in delivering the services, then vendor shall both (a) revoke access to UHS Information, and (b) if the user has access to the UHS Information Systems, either revoke access to the UHS Information Systems if controlled by vendor or otherwise notify UHS, each within one business day of the user no longer requiring access or immediately if the user has been involuntarily terminated.
Infrastructure Protection	Vendor must maintain industry standard controls for the Vendor Information Systems to protect the confidentiality, integrity, availability, and security of UHS Information, including: • physical security controls (including facility and environmental controls) to prevent unauthorized physical access to Vendor Information Systems and areas in which UHS Information is stored or processed, • implementing router filters, firewalls, and intrusion detection and prevention systems to restrict access from public networks to Vendor Information Systems,

	• implementing data loss mechanisms to prevent UHS Information from being moved to unauthorized network locations, • running up-to-date malware prevention and detection software on Vendor Information Systems, • using only applications and operating systems that are still supported by the OEM, • only using software and libraries that are being maintained, • subscribing to receive, and promptly applying, security patches to Vendor Information Systems, • maintaining a register of Vendor Information Systems and tracking of the receipt, removal and transfer of Vendor Information Systems, and • reviewing the security controls at least annually.
Transmitting UHS Information	Vendor must ensure that the electronic transmission or transport on media of UHS Information uses encryption and is performed in a secure manner to prevent unauthorized access or modification.
Cloud Computing	Vendor must notify UHS in advance before using any cloud or shared hosted facilities to store or process UHS Information.
Software Development	If vendor performs software development as part of its services for UHS, vendor must: • follow secure coding and source code management practices, including testing and change management, • use separate development and production environments, • perform code inspections to identify vulnerabilities and malicious code, • ensure that backdoors are not included in the software, and • ensure that processes and documented and implemented for vulnerability management, patching, and verification of security controls before connecting to production networks.