

## STRYKER CORPORATION CASE CARE CLOUD TERMS OF SERVICE ADDENDUM

Last modified: September 17, 2026

These Case Care Cloud Terms of Service Addendum (together with the Stryker Corporation Software and Hosting Terms and Conditions) form the “Agreement” and governs Customer’s access to and use of the Product. This Agreement is entered into by Stryker and the Customer indicated in the applicable Ordering Document.

### 1. DEFINITIONS.

**Access** means access, use, collect, obtain, maintain, handle, process, copy, record, organize, store, host, transmit, transfer, provide, disclose, make available, generate, dispose, erase or destroy.

**Authorized Users** means individuals authorized to use the Products, including employees, Customers, consultants and agents of Customer.

**Case Care Cloud** means the cloud-based, tiered solution enabling Users to collaborate and capture real-time video and photographic images and associated image metadata during surgical procedures, accessible via browser or application.

**Customer Content** means all images, video recordings, files, annotations, labels, patient or procedure information, and associated metadata that Customer or an Authorized User uploads to, records through, stores in, transmits through, or otherwise provides to the Products. Customer Content includes Exported Images before and during transmission through the Products.

**Service Data** means logs, telemetry, session information, device information, usage information, user-experience information, diagnostic information, performance information, and security information generated through the operation or use of the Products. Service Data does not include the substantive content of surgical images, video recordings, audio recordings, or other Customer Content.

**Customer Data** means Customer Content and Service Data to the extent that Service Data identifies Customer, an Authorized User, a patient, or another individual.

**Exported Images** means Customer Content selected by Customer or an Authorized User for transmission from the Products to a Customer-designated EMR System, together with the information and metadata included by Customer in that transmission.

### 2. PROPRIETARY RIGHTS.

**2.1 Stryker Proprietary Rights.** The Software and Subscriptions are licensed and not sold. Stryker and its licensors shall retain ownership of all Software and Subscriptions and all intellectual property rights relating thereto, including but not limited to copyrights, patents, trade secret rights, trademarks and any other intellectual property rights therein. Customer agrees that Stryker may use and exploit without restriction any error reports, suggestions and other information provided by Customer with respect to the Products and shall own any fixes, modifications, improvements and new versions made by Stryker based on such information. The Products, documentation and other non-public information provided by Stryker, and the terms of this Addendum, are confidential to Stryker and its licensors, and shall not be disclosed by Customer to any third party.

**2.2 Customer Proprietary Rights.** Subject to the limited rights expressly granted under the Agreement, Customer retains all right, title, and interest in and to Customer Content and Customer Data, including all related intellectual property rights. Customer grants Stryker and its authorized service providers a worldwide, non-exclusive, royalty-free license during the Term to access, use, reproduce, transmit, store, display, and otherwise process Customer Content and Customer Data as permitted under this Agreement.

For clarity, Customer’s ownership of Customer Content and Customer Data does not limit Stryker’s ownership of or rights in Stryker Data, including service telemetry, diagnostic information, performance information, security information, and data that has been aggregated or de-identified so that it does not identify Customer, an Authorized User, a patient, or any other individual. If there is a conflict between this Section 2.2 and the Stryker Data provisions of the Software and Hosting Terms, this Section 2.2 will control solely with respect to identifiable Customer Content and Customer Data processed through Case Care Cloud.

**2.3 Data Use.** Stryker may process Customer Content and identifiable Customer Data only to provide, secure, support, maintain, administer, and improve the Products for Customer; comply with Customer’s documented instructions; enforce the Agreement; and comply with applicable law.

Stryker may generate and use Service Data arising from the operation or use of the Products. Stryker may use Service Data in identifiable form for security, support, diagnostic, service-performance, fraud-prevention, contract-administration, and legal-compliance purposes. Stryker may use Service Data and Customer Data for broader analytics, benchmarking, research, product development, and artificial-intelligence or machine-learning development only where the information has been

aggregated or de-identified in accordance with applicable law so that it does not identify Customer, an Authorized User, a patient, or any other individual, or where Customer has separately authorized such use in writing.

Stryker will not sell Customer Content or use identifiable Customer Content to advertise or market third-party products. Stryker will not attempt to re-identify aggregated or de-identified information except as permitted by law to evaluate or validate the effectiveness of the de-identification process.

**2.4 Third Party Components.** The Products may contain certain third-party components provided under terms and conditions different from those set forth in this Addendum, and Customer agrees that all such third-party components will be subject to such other terms and conditions to the extent inconsistent with this Agreement, or to the extent required by such other terms and conditions. All implied licenses are disclaimed, and all rights not expressly granted herein are reserved to Stryker or its licensors.

### 3. CUSTOMER OBLIGATIONS

**3.1 Permitted Uses.** Stryker hereby grants to Customer a non-exclusive, worldwide, royalty-free limited right during the Term to allow access to, and use of, the Products by authorized Users solely for Customer's internal business purposes. Customer may change users or allow use to other or additional authorized Users, all within the scope of the applicable Ordering Document. Customer shall be responsible for all acts and omissions associated with the access and use of the Products through Customer's account by its users. Customer may use the Products only in accordance with this Addendum. Customer may not reverse engineer, decompile, disassemble, or work around technical limitations in the Products, except to the extent applicable law permits it despite these limitations. Customer may not disable, tamper with, or otherwise attempt to circumvent any billing mechanism that meters Customer's use of the Products. Customer may not rent, lease, lend, resell, transfer, or host the Product, or any portion thereof, to or for third parties except as expressly permitted in this Addendum or the Services Terms.

**3.2 Authorized Users.** Customer shall control access by its Authorized Users, and Customer shall be responsible for their use of the Products in accordance with the terms of this Addendum.

**3.3 Restrictions.** Except as otherwise may be provided in the Agreement, Customer shall not: (i) rent, lease, sell, or sublicense the Products to an unauthorized third party; (ii) use the Products to provide service bureau or timesharing professional services; (iii) interfere with any license key mechanism in the Products; (iv) reverse engineer, disassemble, decompile, translate, or otherwise seek to derive the source code for the Products; or (v) use the Products in order to develop a similar or competitive product or service to the Products. All media files and content uploaded, stored, administered, edited, delivered, made available, distributed or otherwise provided by Customer in connection with its use of Products ("**Customer Content**") are solely Customer's responsibility. Without limiting the foregoing, Customer will not transmit, display, distribute or otherwise make available through the Products content that is illegal, harmful, obscene, pornographic, defamatory, libelous, abusive, harassing, threatening, fraudulent, infringes upon a third-party's intellectual property or privacy rights, or may damage, interfere with, or expropriate the Products or any third party's system or program. Stryker may, but is under no duty to, review Customer Content and remove or block access to such content via the Products, if Stryker, in its sole discretion, has reasonable grounds to believe or receives a notice from a third party, that such content may violate the restrictions set forth in this Section. Stryker will use reasonable efforts to provide Customer with a notice at least forty-eight (48) hours prior to final removal of said content from the Products.

### 4. SUSPENSION.

Stryker may suspend affected use immediately where Stryker reasonably determines that use of the Services creates an imminent security, legal, patient-safety, or operational risk, or where suspension is required by law. For other violations, Stryker will provide notice and a reasonable opportunity to cure, not to exceed five business days, before suspension. Stryker will limit any suspension to the affected portion of the Products where reasonably practicable and will restore access after the violation has been remedied.

### 5. DISCLAIMER OF WARRANTIES

**Warranty Disclaimer.** STRYKER MAKES NO WARRANTIES, EXPRESS OR IMPLIED, OTHER THAN THOSE EXPRESSLY SET FORTH IN THIS AGREEMENT, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTIES ARISING FROM USAGE OF TRADE OR COURSE OF DEALING OR PERFORMANCE.

### 6. STORAGE OF CUSTOMER DATA.

During the Subscription Term, Stryker will retain Customer Content in accordance with the applicable Ordering Document and Product Documentation. Following expiration or termination, Stryker will make Customer Content available for retrieval for one hundred and twenty days, unless a different period is stated in the Ordering Document. After that period, Stryker may delete or render Customer Content unrecoverable from active systems. Customer Content remaining in backups will be deleted or overwritten in accordance with Stryker's ordinary backup-retention cycle, except to the extent retention is required by law or an applicable legal hold.

## 7. EXPORT TO EMR SYSTEMS.

**7.1** The Products enable Customer to export images and related information ("**Exported Images**") to Customer-designated electronic medical record or other clinical systems ("**EMR Systems**"). Stryker shall maintain the integrity and security of Exported Images while processed and transmitted by the Products through successful transmission to the applicable EMR System, in accordance with this Agreement and in accordance with the applicable Business Associate Agreement.

**7.2** Customer is responsible for configuring and maintaining its EMR Systems and third-party interfaces, selecting the appropriate destination and patient record, and verifying successful receipt and association of Exported Images with the correct patient and surgeon record(s). Following successful transmission, Stryker shall not be responsible for the operation of an EMR System or for any other loss, alteration, duplication, misrouting, or other issues arising within the EMR System or a third-party interface, except to the extent caused by Stryker or the Products.

## EXHIBIT A SECURITY TERMS AND CONDITIONS

This Security Terms and Conditions Exhibit (the "**Security Exhibit**") is incorporated into and forms part of the Stryker Software and Hosting Terms and Conditions (the "**Software and Hosting Terms**") and the Agreement. All capitalized terms not defined herein have the meanings given in the Software and Hosting Terms. In the event of conflict between this Security Exhibit and the Software and Hosting Terms or the Agreement, this Security Exhibit will control with respect to its subject matter. Security controls described in Product Documentation, a Data Processing Agreement, and any relevant Product Addendum will control in the event of conflict with this Security Exhibit.

### 1. DEFINITIONS

**Security Incident** means a confirmed breach of security leading to unauthorized access to, acquisition of, loss of, or disclosure of Customer's Content within Stryker's control that compromises its confidentiality, integrity, or availability.

**SBOM** means a software bill of materials describing the software components of Stryker Software, in a format determined by Stryker in its reasonable discretion.

**Vulnerability** means a weakness in Stryker Software that, if exploited, could reasonably be expected to compromise the confidentiality, integrity, or availability of a Product or Customer's Content.

### 2. INFORMATION SECURITY PROGRAM

Stryker has established and will maintain a written information security program that includes administrative, technical, and physical safeguards reasonably designed to protect against the destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Customer's Content within Stryker's possession or control. Stryker will use appropriate technical and organizational measures to protect Customer Content, such as those described in Appendix 1 to this Security Exhibit ("**Security Measures**"). Stryker may modify or update these Security Measures, provided that such updates do not materially reduce the overall security of the Products or Customer's Content.

### 3. SECURE DEVELOPMENT

Stryker maintains commercially reasonable secure development practices designed to identify and remediate material known Vulnerabilities in Stryker Software prior to release. As appropriate to the nature of the Product, such practices may include threat modeling, secure coding practices, vulnerability scanning, SBOM maintenance, and pre-release security testing. Security capabilities for Products are described in applicable Product Documentation. Personnel with software development responsibilities periodically receive training in secure development practices.

### 4. VULNERABILITY MANAGEMENT

Stryker maintains a Vulnerability management program that, as appropriate to each Product, includes monitoring of public vulnerability sources, coordinated disclosure procedures, and risk-prioritized handling of identified Vulnerabilities. Stryker will make available security updates and patches to address Vulnerabilities in Stryker Software in accordance with the Agreement and Product Documentation or as otherwise notified in writing. Stryker may, in its reasonable discretion, prioritize Vulnerabilities based on factors including severity and exploitability, the population of affected Products, the availability of effective compensating controls, the nature and intended use of the Product, and applicable regulatory requirements. For Products that incorporate third-party software, Stryker's commitments under this Section are subject to the availability of security updates from the relevant third-party supplier.

### 5. INCIDENT RESPONSE

Stryker maintains a written incident response program for Hosting Services that includes processes for detection, triage, containment, eradication, recovery, and post-incident review. Stryker will notify Customer without undue delay after becoming aware of a Security Incident, in accordance with applicable law. Stryker will investigate the Security Incident and provide Customer with relevant information about the Security Incident, as required under applicable laws. Stryker will use reasonable efforts to assist the Customer in mitigating, where possible, the adverse effects of a Security Incident. Stryker's notification to Customer of a Security Incident will not be deemed an acknowledgment of fault or liability.

### 6. DOCUMENTATION

Upon Customer's written request no more frequently than once every twelve (12) months and subject to confidentiality obligations, Stryker will provide to Customer information reasonably necessary to demonstrate its compliance with this Security Exhibit. Stryker may satisfy this obligation by providing Customer with such industry standard security certifications, attestations, audit reports, SBOMs and Manufacturer Disclosure Statements for Medical Device Security for regulated medical devices, and similar documentation as Stryker maintains in the ordinary course of business for applicable Products, in formats determined by Stryker.

### 7. CUSTOMER RESPONSIBILITIES

In addition to the responsibilities set forth in the Software and Hosting Terms, Customer will, at Customer's expense:

- (a) Implement and maintain commercially reasonable security measures in Customer's environment, including network segmentation, perimeter protections, endpoint protections, identity and access management, and physical security, consistent with Product Documentation;
- (b) Ensure that the operating environment for any Customer-Hosted Software and any infrastructure used to connect to Stryker-Hosted Software or Hosting Services satisfies the requirements set forth in the Product Documentation;
- (c) Configure and use the Stryker Software and Hosting Services in accordance with the Product Documentation and any baseline security configurations made available by Stryker;
- (d) Timely install Updates, security updates, and patches made available by Stryker; and
- (e) Promptly notify Stryker of any suspected Security Incident or Vulnerability affecting the Stryker Software or Hosting Services of which Customer becomes aware, and reasonably cooperate with Stryker in connection with any investigation.

Stryker has no obligation to correct, cure, or otherwise remedy any error, defect, Vulnerability or Security Incident resulting from

(1) modifications to Stryker Software, firmware, or programmable hardware by any person not authorized by Stryker; (2) Customer's breach of the foregoing responsibilities; (3) acts or omissions of Customer, its personnel, subcontractors, agents, Users, or any third party not under Stryker's control; or (4) any cause outside of Stryker's reasonable control.

#### **8. MISCELLANEOUS**

Stryker may perform any of its obligations under this Security Exhibit directly or through its affiliates, provided that Stryker remains responsible for such performance. Customer's sole and exclusive remedy for any breach of Stryker's warranties or obligations contained herein shall be, at Stryker's option and using commercially reasonable efforts: (a) to correct, remediate, patch, or update the applicable nonconformity within a reasonable period of time; or (ii) in Stryker's sole discretion, to repair or replace the affected Product with software or services that provide substantially equivalent functionality in all material respects. This Security Exhibit will survive termination or expiration of the Agreement to the extent necessary to give effect to their purpose, consistent with Section 11 of the Software and Hosting Terms. Headings are for convenience only and do not affect interpretation. Qualifiers are material to the parties' allocation of risk and will be given full effect in any interpretation of this Security Exhibit. All obligations of Stryker under this Security Exhibit are subject to the limitations of liability, disclaimers, and exclusions set forth in the Agreement.

## APPENDIX 1 SECURITY MEASURES

This Appendix describes Stryker's Security Measures for safeguarding Customer Content that is processed within Stryker's enterprise infrastructure and Stryker Hosting Services. Product-specific supplements to these Security Measures may be outlined in Product Documentation or Product Addenda.

| Domain                                    | Practices                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Security Program</b>                   | <ul style="list-style-type: none"> <li>• Documented information security policies, reviewed and approved by management on a periodic basis.</li> <li>• Periodic management review of the program, including risk assessments, audit results, and incidents.</li> <li>• Chief Information Security Officer accountability for information security program.</li> <li>• Recurring internal review of the information security management system.</li> <li>• Periodic testing and evaluation of the effectiveness of the Security Measures.</li> </ul>                                                                                                                                                                              |
| <b>Personnel Security</b>                 | <ul style="list-style-type: none"> <li>• Background screening for employees, based on role and sensitivity, where permitted under applicable law.</li> <li>• Information security and privacy awareness training upon hire and on a recurring basis aligned to an individual's role.</li> <li>• Written confidentiality obligations applicable to personnel with access to Customer's Content.</li> <li>• Remote-working policies and procedures governing secure access to Stryker systems and networks from outside Stryker facilities.</li> <li>• Account de-provisioning processes upon employee exit or termination.</li> <li>• Documented disciplinary process for violations of information security policies.</li> </ul> |
| <b>Physical Security</b>                  | <ul style="list-style-type: none"> <li>• Control of secure areas through access-control mechanisms, monitoring, and authorization procedures.</li> <li>• Utilization of security cameras and security guards, where necessary.</li> <li>• Physical access requirements applicable to third parties and visitors documented and contractually imposed where relevant.</li> <li>• Documented procedures for the secure disposal of physical media containing Customer's Content.</li> </ul>                                                                                                                                                                                                                                        |
| <b>Vendor and Supply Chain Management</b> | <ul style="list-style-type: none"> <li>• Due diligence prior to engaging any third party that will access Stryker networks or Customer Content.</li> <li>• Incorporation of information security and privacy requirements into supplier agreements, where required.</li> <li>• Confidentiality agreements for third parties with access to Stryker networks.</li> <li>• Periodic monitoring and review of supplier services.</li> <li>• Maintenance of SBOMs for applicable Products.</li> </ul>                                                                                                                                                                                                                                 |
| <b>Product Security</b>                   | <ul style="list-style-type: none"> <li>• Integration of appropriate security and privacy controls into the design, development, and operation of Products.</li> <li>• Threat modeling and pre-release security testing during product development.</li> <li>• Secure coding practices informed by recognized industry frameworks, including OWASP Top 10 for web applications and IEC 81001-5-1 for medical devices.</li> </ul>                                                                                                                                                                                                                                                                                                  |

| Domain                          | Practices                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Access Controls</b>          | <ul style="list-style-type: none"> <li>• Access to information assets managed in accordance with least-privilege and need-to-know principles.</li> <li>• Centralized identity and access management for enterprise-managed resources through directory services and single sign-on, where supported by the system architecture.</li> <li>• Password complexity requirements, minimum length, and periodic expiration consistent with industry practice.</li> <li>• Multi-factor authentication for administrative access to Hosting Services processing Customer's Content.</li> <li>• Automatic session lockout following a defined period of inactivity or failed authentication attempts.</li> <li>• Periodic user identity and access rights reviews by systems owners.</li> <li>• Segregation of duties to prevent conflicting roles assigned to the same individual.</li> <li>• Logical or physical segregation of production and development environments.</li> </ul> |
| <b>Data Protection</b>          | <ul style="list-style-type: none"> <li>• Designated privacy accountability and records of processing activities.</li> <li>• Processing of personal data consistent with Customer's instructions and the minimum reasonably needed to provide the Products and Hosting Services.</li> <li>• Processes designed to facilitate personal data accuracy.</li> <li>• Reasonable assistance with Customer's privacy risk assessments.</li> <li>• Return or deletion of personal data on Customer request or termination, subject to retention obligations.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Change Management</b>        | <ul style="list-style-type: none"> <li>• Documented change-management procedures for production environments.</li> <li>• Production data is not used in test environments without appropriate safeguards.</li> <li>• Testing and validation of software updates and patches prior to deployment.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Encryption</b>               | <ul style="list-style-type: none"> <li>• Documented cryptographic controls to protect the confidentiality and integrity of data according to sensitivity.</li> <li>• Encryption in transit over public or untrusted networks.</li> <li>• Encryption at rest for Stryker-managed servers storing Customer's Content.</li> <li>• Pseudonymization of personal data, where appropriate.</li> <li>• Encrypted VPN for remote administrative access to Hosting Services processing Customer's Content.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Business Continuity</b>      | <ul style="list-style-type: none"> <li>• Routine backup of Hosting Systems according to documented frequencies.</li> <li>• Data replication across data centers or geographies, depending on criticality.</li> <li>• Business continuity and disaster recovery plans for critical systems.</li> <li>• Monitoring of system availability and integrity, with defined alerting for malfunctions and degradations.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Configuration Management</b> | <ul style="list-style-type: none"> <li>• Primary and supporting information assets inventoried, tracked, and reviewed by designated personnel on a periodic basis.</li> <li>• Configuration Management Database to manage relationships among information system components.</li> <li>• Asset and data classification according to sensitivity criteria.</li> <li>• Acceptable use rules defined and communicated to employees, contractors, and third parties, and reviewed periodically.</li> <li>• Hardening standards and secure configuration checklists applicable to the deployment of information systems and service accounts.</li> </ul>                                                                                                                                                                                                                                                                                                                           |
| <b>Vulnerability Management</b> | <ul style="list-style-type: none"> <li>• Formal risk-management methodology to identify, assess, treat, and monitor information security risks.</li> <li>• Vulnerability scans and penetration testing performed prior to release of applicable Products.</li> <li>• Monitoring of public and industry vulnerability sources on an ongoing basis.</li> <li>• Vulnerabilities scored using the Common Vulnerability Scoring System (CVSS).</li> <li>• Documented Coordinated Vulnerability Disclosure program.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Domain                     | Practices                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Incident Management</b> | <ul style="list-style-type: none"> <li>• Documented incident response plan, procedures and work instructions.</li> <li>• A documented major-incident communication process defining internal roles and timing for status updates throughout the incident lifecycle.</li> <li>• Continuous security monitoring of systems, with defined escalation procedures to Stryker's Cybersecurity Incident Response Team.</li> <li>• Severity classification for product security based on impact to product function, patient safety, data, and recoverability.</li> <li>• Audit logging of activities involving Customer's Content, retained for a defined period for investigative purposes.</li> </ul> |
| <b>Endpoint Protection</b> | <ul style="list-style-type: none"> <li>• Anti-malware and endpoint protection and response tools deployed on Stryker-managed endpoints and servers used to process Customer's Content.</li> <li>• Full-disk encryption on Stryker-managed laptops and mobile devices.</li> <li>• Centralized management of endpoint configuration and security agents.</li> </ul>                                                                                                                                                                                                                                                                                                                                |