
HealthStream®

myClinicalExchange Order Form

HealthStream®

Effective Date March 6, 2024

Order Number ORD-0797640
P.O. Number
Tax Exempt? No

Customer Information
Name Saguaro High School- Scottsdale Unified School District
Address 6250 N. 82nd St.
Scottsdale, AZ 85250

Primary Contact
Name Bailey Ricard
Email bricard@susd.org
Phone 480-484-5018

Billing Contact
Name Bailey Ricard
Email bricard@susd.org
Phone 480-484-5018

HealthStream Information
Name HealthStream, Inc.
Address 500 11th Avenue North
Suite 1000
Nashville, TN 37203

ORDER DETAILS – The pricing set forth in this Order Form, including any applicable discounts, shall expire if this Order Form is not signed and returned to HealthStream on or before 5:00PM Central Time on March 21, 2024.

Billing Frequency: Quarterly

Product	Quantity of Users	Unit Price (per user per year)	Term	Total
myClinicalExchange B2B Higher Ed	1	$0.00	12	$0.00
myClinicalExchange - B2C (Individual - Academic Instructor)	1	$0.00	12	$0.00

Total: $0.00

This Order Form, along with the Part A – Product Descriptions and Part B – Terms and Conditions, as well as the Security Addendum incorporated herein as Part C, is entered into and effective as of the Effective Date by and between HealthStream, Inc., a Tennessee corporation, having its principal place of business at 500 11th Avenue North, Suite 1000, Nashville, Tennessee 37203 ("HealthStream") and Saguaro High School- Scottsdale Unified School District, located at 6250 N. 82nd St. Scottsdale, AZ 85250(“Customer").

PART A
PRODUCT DESCRIPTION

Product Specific Terms

myClinicalExchange (Enterprise)
myClinicalExchange assists facilitators with the process of launching, educating, and management of students and instructors throughout the clinical placement process.

myClinicalExchange product features include:

- Using a single platform to manage multiple programs and placements
- Web-based training for healthcare organizations and academic institutions included at no additional cost
- Tracking of all placement requests in real-time
- Availability to view and approve placement requests
- The ability to differentiate preceptorships, internships, cohorts, volunteers, etc.
- The ability to customize online orientation and testing process
- The ability to customize assessments/surveys
- The ability to customize rotational compliance checklist by Program, Department, Unit, etc.
- Management of students' compliance status (checklist, documents, orientation, etc.)
- Receipt of contextual email alerts

Minimum Technical Specifications

- Laptops, Desktops with Windows /MAC preferably most versions.
- Internet Explorer 11 and above, Google Chrome, and Firefox. Google Chrome is recommended.
- Internet connection with 1 Mbps and above.

Billing
Subscription rates for Users/Instructors are as follows:

- User: $39.50 per year or $20.00 for a six month term
- Academic Instructor: $21.50 per year

Billing by HealthStream will be issued quarterly based on monthly usage at the rates set forth above.

This Order Form commences on the Effective Date and continues through the term set forth in the Order Details above (the "Initial Term"). This Order Form shall renew for additional one (1) year terms (each, a "Renewal Term), unless either party provides notice of non-renewal at least ninety (90) days prior to the end of the applicable Term. The Initial Term and each Renewal Term shall collectively be referred to as the "Term". Notwithstanding anything to the contrary, HealthStream reserves the right to increase the fees due under this Order Form effective as of January 1st of each calendar year. Upon the publishing of a fee increase by HealthStream, Customer shall have the right to terminate this Order Form without penalty, within ninety (90) days of the publishing of the price increase by HealthStream.

myClinicalExchange Program
Notwithstanding the provisions set forth in the MSA (as defined herein), the Quantity set forth in the Order Details above reflects total number of "Programs" being managed on the Customer's behalf on an annual basis. A "Program" shall mean a category of education and training that is offered at the clinical site managed by the MyClinicalExchange Product.

my Clinical Exchange - B2C (Individual – Academic Instructor)
mCE assists facilitators with the process of launching, educating, and management of students and instructor compliance status throughout the clinical placement process.

mCE product features include:

- Using a single platform to manage multiple programs and placements
- Web-based training for healthcare organizations and academic institutions included at no additional cost
- Tracking of all placement requests in real-time
- Availability to view and approve placement requests
- The ability to differentiate preceptorships, internships, cohorts, volunteers, etc.
- The ability to customize online orientation and testing process
- The ability to customize assessments/surveys
- The ability to customize rotational compliance checklist by Program, Department, Unit, etc.
- Management of students' and instructors' compliance status (checklist, documents, orientation, etc.)
- Receipt of contextual email alerts

Minimum Technical Specifications

- Laptops, Desktops with Windows /MAC preferably most versions.
- Internet Explorer 11 and above, Google Chrome, and Firefox. Google Chrome is recommended.
- Internet connection with 1 Mbps and above.

Payment Terms
The Customer will not pay HealthStream as the instructors will pay the following fees directly to HealthStream: 12 Month Subscription: $21.50

Notwithstanding the provisions set forth in the MSA (as defined herein), the Quantity set forth in the Order Details above reflects total number of "Programs" being managed on the Customer's behalf on an annual basis. A "Program" shall mean a category of education and training that is offered at the clinical site managed by the MyClinicalExchange Product.

Customer acknowledges and agrees that HealthStream has the Customer's authority and permission to provide Customer Data to educational institution(s) with whom Customer has an Affiliation Agreement ("Educational Institutions") by linking the Educational Institution's mCE profile to Customer's mCE profile, upon Customer's request. Customer shall to the extent permitted by law, defend, indemnify and hold HealthStream and its officers, directors, employees, licensors, representatives and/or agents harmless at all times from and against any and all claims, demands, actions, proceedings, damages, losses, liabilities, costs, and/or expenses (including without limitation, reasonable attorneys fees) in connection with or as a result of any claim that arises from the provision of the Customer Data by HealthStream to Educational Institutions at Customer's request.

This Order Form commences on the Effective Date and continues through the term set forth in the Order Details above (the "Initial Term"). This Order Form shall renew for additional one (1) year terms (each, a "Renewal Term), unless either party provides notice of non-renewal at least ninety (90) days prior to the end of the applicable Term. The Initial Term and each Renewal Term shall collectively be referred to as the "Term". Notwithstanding anything to the contrary, HealthStream reserves the right to increase the fees due under this Order Form effective as of January 1st of each calendar year. Upon the publishing of a fee increase by HealthStream, Customer shall have the right to terminate this Order Form without penalty, within ninety (90) days of the publishing of the price increase by HealthStream.

Facilities & Programs

Programs:

1 Program

Nursing Assistant (Students & Instructors)

PART B
TERMS AND CONDITIONS

Section 1 – Definitions

1.1 "Online Service(s)" means the Products set forth herein and provided by HealthStream to Customer.

1.2 "Users those who are authorized by Customer to use the Online Service(s) and have been supplied user identifications and passwords by Customer (or by HealthStream at Customer's request).

Section 2 – Responsibilities

2.1 HealthStream Responsibilities. Subject to the terms of this agreement, HealthStream shall provide the Online Services described in Part A. HealthStream shall use commercially reasonable efforts to make the Online Service(s) generally available 24 hours a day, 7 days a week, except for: (i) planned downtime; or (ii) any unavailability caused by circumstances beyond HealthStream's reasonable control, including without limitation, acts of God, acts of government, flood, fire, earthquakes, civil unrest, acts of terror, strikes or other labor problems (other than those involving HealthStream employees), computer, telecommunications, Internet service provider or hosting facility failures or delays involving hardware, software or power systems not within HealthStream's possession or reasonable control, and network intrusions or denial of service attacks.

2.2 Customer Responsibilities. Customer is responsible for all activities that occur under Customer's User accounts. Customer shall: (a) have sole responsibility for the accuracy, quality, integrity, legality, reliability, and appropriateness of all Customer Data; (b) use commercially reasonable efforts to prevent unauthorized access to, or use of, the Service(s), and notify HealthStream promptly of any unauthorized use; (c) use the Services for its internal business purposes only; and (d) comply with all applicable local, state, federal, and foreign laws in using the Service(s) and, if using the Service(s) outside of the United States, not use the Service(s) in a manner that would violate any federal or state laws of the United States if conducted in the United States. Customer is solely responsible for providing support to Users. HealthStream shall provide remote technical assistance solely to Customer's designated representative.

Section 3 – Intellectual Property and Data

3.1 License Grant. HealthStream grants Customer and its Users a worldwide, non-exclusive, non-transferable, non-sublicenseable right to access and use the Service(s) in accordance with the terms of this Agreement.

3.2 Restrictions. Customer shall not (a) modify, copy or create derivative works based on the Service(s) or HealthStream IP; (b) create Internet "links" to or from the Service(s), or "frame" or "mirror" any content forming part of the Service(s), other than on Customer's own intranet; or (c) disassemble, reverse engineer, or decompile the Service(s) or HealthStream IP, or access it in order to build a similar or competitive product or service or copy any ideas, features, functions or graphics of the Service(s). The HealthStream IP is covered by intellectual property rights owned or licensed by HealthStream. For purposes of this Agreement, "HealthStream IP" means (a) the HealthStream name, the HealthStream logo, the HealthStream domain name, the product and service names associated with the Service(s), and other trademarks and service marks; (b) certain audio and visual information, documents, software and other works of authorship; (c) certain processes including, but not limited to, HealthStream's databases, questionnaires, market research procedures, tabulation procedures, creative processes, statistical methods, and production methods; and (d) other technology, software, hardware, products, processes, algorithms, user interfaces, know-how and other trade secrets, techniques, designs, inventions and other tangible or intangible technical material or information.

3.3 Customer Data. As between HealthStream and Customer, all data obtained by HealthStream from Customer through the provision of the Service(s) (collectively, the "Customer Data") is owned exclusively by Customer. Customer grants HealthStream an unrestricted, royalty-free, irrevocable license to maintain and distribute de-identified aggregated compilations of the Customer Data ("Aggregated Data") and to use such Aggregated Data for future studies and reports; provided, however, that the Aggregated Data will not reveal any personal information or the identity of Customer or any User. HealthStream may distribute certain Customer Data to licensing and accreditation organizations for the benefit of Users. HealthStream will release the minimum data required to adequately credit Users for educational activities completed.

3.4 Definition of Confidential Information. As used in this Agreement, and, subject to any public records laws applicable to Customer, "Confidential Information" means all confidential and proprietary information of a party ("Disclosing Party") disclosed to the other party ("Receiving Party"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure including, without limitation, this Order Form, the Customer Data, the Online Service(s), and HealthStream's business and marketing plans, technology and technical information, product designs, and business processes. Confidential Information (except for Customer Data) shall not include any information that: (a) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party; (b) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party; (c) was independently developed by the Receiving Party without breach of any obligation owed to the Disclosing Party; or (d) is received from a third party without breach of any obligation owed to the Disclosing Party.

3.5 Confidentiality. Subject to Arizona Public Records law as applicable, the Receiving Party shall not disclose or use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Order Form. Each party agrees to protect the confidentiality of the Confidential Information of the other party in the same manner that it protects the confidentiality of its own proprietary and confidential information of like kind, but in no event shall either party exercise less than reasonable care in protecting the Confidential Information. Subject to any public records laws applicable to Customer, if the Receiving Party is compelled by law to disclose Confidential Information of the Disclosing Party, it shall provide the Disclosing Party with prior notice of the compelled disclosure (to the extent legally permitted) and reasonable assistance, at Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure.

Section 4 – Warranties and Indemnification

4.1 General. Each party represents and warrants that it has the legal power to enter into this Agreement. HealthStream represents and warrants that (i) it will provide the Service(s) in a manner consistent with general industry standards reasonably applicable to the provision of the Service; and (ii) it owns or otherwise has sufficient rights to the Service(s) and the HealthStream IP to grant the rights and licenses granted in this Agreement. Customer agrees that its purchase of the Service(s) is not contingent upon the delivery of any future functionality or features nor is it dependent upon any oral or written public comments made by HealthStream with respect to future functionality or features.

4.2 Disclaimer. EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT, HEALTHSTREAM MAKES NO WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE. HEALTHSTREAM SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

4.3 Limitation of Liability and Exclusion of Damages. IN NO EVENT SHALL EITHER PARTY'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, EXCEED THE LESSER OF $100,000 OR THE AMOUNTS ACTUALLY PAID BY AND DUE FROM CUSTOMER UNDER THIS AGREEMENT. IN NO EVENT SHALL EITHER PARTY HAVE ANY LIABILITY TO THE OTHER PARTY FOR ANY LOST PROFITS, LOSS OF USE, COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES HOWEVER CAUSED AND, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF THE DAMAGE.

Section 5 – Term and Termination

5.1 Term. This Agreement commences on the Effective Date and continues through the term set forth in the Order Details above (the "Term").

5.2 Termination. A party may terminate this Agreement for cause: (a) upon forty-five (45) days written notice of a material breach to the other party if the breach remains uncured at the expiration of the thirty-day cure period; or (b) if the other party becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors. Termination shall not relieve Customer of the obligation to pay any fees accrued or payable to HealthStream prior to the effective date of termination.

Section 6 – General

6.1 Payments. HealthStream shall invoice Customer per the Order Details or Product Description(s) above and all invoices shall be due and owed when they are received. For invoices that are greater than thirty days past due, HealthStream reserves the right to suspend services.

6.2 Privacy. In the event that HealthStream receives student data or information that is subject to the Family Educational Rights and Privacy Act ("FERPA") then HealthStream shall comply with all applicable guidelines.

6.3 Notices. Notices under this Agreement shall be sent overnight delivery via nationally recognized courier shall be deemed delivered upon receipt as confirmed by delivery confirmation. Notices to HealthStream shall be addressed to the attention of its Legal Department.

6.4 Waiver and Cumulative Remedies; Severability. No failure or delay by either party in exercising any right under this Agreement shall constitute a waiver of that right. Other than as expressly stated in this Agreement, the remedies provided in the Agreement are in addition to, and not exclusive of, any other remedies of a party at law or in equity. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision shall be modified by the court and interpreted so as best to accomplish the objectives of the original provision to the fullest extent permitted by law, and the remaining provisions of this Agreement shall remain in effect.

6.5 Surviving Provisions. The following provisions shall survive any termination or expiration of this Agreement: 3 (excluding Section 3.1), 4, and 6.

6.6 Jury Trial Waiver. Each party waives any right to jury trial in connection with any action or litigation in any way arising out of or related to this Agreement.

IN WITNESS WHEREOF, and intending to be legally bound hereby, each party hereto warrants and represents that this Order Form has been duly authorized by all necessary corporate action and that this Order Form has been duly executed by and constitutes a valid and binding agreement of that party.

HealthStream Inc.

By: Deborah B. Shapiro
Deborah B. Shapiro (Mar 6, 2024 17:13 EST)

Print Name: Deborah B. Shapiro

Print Title: Senior Counsel

Date: Mar 6, 2024

Saguaro High School- Scottsdale Unified School District

By: Nicholas B. Buzan
Nicholas B. Buzan (Mar 6, 2024 15:21 MST)

Print Name: Nicholas B. Buzan

Print Title: General Counsel

Date: Mar 6, 2024

Part C
Information Security Addendum

HealthStream, Inc. shall be referred to herein as "we", "us" or "our". This Security Addendum is incorporated into and made a part of the written agreement between the parties that references this document (the "**Agreement**") and any capitalized terms used but not defined herein shall have the meaning set forth in the Agreement. In the event of any conflict between the terms of the Agreement and this Security Addendum, this Security Addendum shall govern.

We maintain a comprehensive documented security program based on NIST CSF framework (or industry recognized successor framework), under which we implement and maintain physical, administrative, and technical safeguards designed to protect the confidentiality, integrity, availability, and security of the Online Services and Customer Data (the "**Security Program**"), including, but not limited to, as set forth below. We regularly test and evaluate our Security Program and may review and update its Security Program as well as this Security Addendum, provided, however, that such updates shall be designed to enhance and not materially diminish the Security Program.

The Security Program and its policies and procedures cover all of our workforce members, including full- time and part-time employees in all job roles, temporary staff, contractors and subcontractors, volunteers, interns, managers, executives, employees, and third parties.

1. Hosting Locations.

1.1. We host our mission-critical servers in dedicated cages within data centers located in the US. These data centers are ISO 27001, SOC1, and SOC2 compliant.

1.2. These facilities feature 24/7 manned security, fully redundant power backup systems, physical access controls, biometric authentication systems, extensive seismic bracing, the latest in early-detection smoke and fire alarms, and digital surveillance systems. All server and network components are continuously monitored by internal staff and by the colocation providers.

1.3. Access to each system, network device, and application is limited to authorized personnel, and login details within the event logs are reviewed on a continual basis.

2. Data Protection and Backup. Our data backup model provides near real-time database replication to ensure Customer Data is both backed up and available on redundant and geographically dispersed servers. Full back up is performed on a daily basis and is stored encrypted in an environment physically separated from the primary servers to ensure fault tolerance.

3. Disaster Recovery. We maintain a replicated backup hosting facility in both our cloud and on-prem hosting. All production data is fully replicated to a redundant and geographical dispersed hosting facility. Disaster Recovery plans are tested on an annual basis.

4. Data Encryption. We use Transport Layer Security (TLS) 1.2 with a preferred AES 256-bit algorithm in CBC mode and 2048-bit server key length with industry-leading modern browsers. When an individual accesses our platform via web browser, mobile applications, email add-in, or browser extension, TLS technology protects that information using data encryption.

5. Network Security. We use industry-standard network protection procedures, including network segregation using VLAN's, firewall and router technologies, intrusion detection and prevention systems, centralized log aggregation, and alert mechanisms. These procedures are used in conjunction with secure connectivity, including secure channels and multi-factor authentication for authorized systems operations group personnel. This allows us to prevent, detect, and promptly remediate the impact of malicious traffic and network attacks.

6. Regular Updates and Patch Management. Ongoing internal network security audits and scanning gives us an overview for quick identification of impacted systems and services. According to our corporate patch management policy, operating systems, software, frameworks, and libraries used in our infrastructure are updated to the latest versions on a regular basis. Whenever a vulnerability in a product used by us or a high or critical vulnerability is publicly reported, prompt actions are taken to mitigate any potential risks for our customers — including the application of hotfixes and patches promptly when available and/or implementing pro-active compensating controls such as configuration of firewalls or IDS/IPS.

7. Separation of Customer Data. Customer Data is logically separated at the database/datastore level using a unique identifier for the institution.

8. Security Incident Reporting and Response. We implement an information security incident response process to consistently detect, respond, and report incidents, minimize loss and destruction, mitigate the weaknesses that were exploited, and restore information system functionality and business continuity as soon as possible.

8.1. The incident response process addresses:

- Continuous monitoring of threats through intrusion detection systems and other monitoring applications.
- Establishment of an information security incident response team.
- Establishment of clear procedures for identifying, responding, assessing, analyzing, and follow-up of information security incidents.
- Workforce training, education, and awareness on information security incidents and required responses.
- Facilitation of clear communication of information security incidents with internal, as well as external, stakeholders, as required.

9. User Authentication. Each user in our platform has a unique, password-protected account with a verified email address. The password is validated against password policies and stored securely using a strong hashing algorithm with a unique salt for every password. We also support multiple methods of federated authentication, including PING Identity SSO, OAUTH and SAML2 to gain access conveniently and securely to a platform account for customer authentication.

10. Access Controls.

10.1. Access. Employee access to production is guarded by an approval process. When access is approved, temporary

access is granted that allows access to production. Production access is reviewed by the security team on a case-by-case basis.

10.2. Need-to-Know and Least Privilege. Only a limited set of employees have access to our datacenter and the data stored in our databases. There are strict security policies for employee access, all security events are logged and monitored, and our authentication methods and data are strictly regulated. Access to production requires establishing a VPN channel, multi-factor authentication and a secure username and password. We limit access to customer data to employees with a job-related need and require all these staff members to sign a confidentiality agreement. Accessing Customer Data is only done on an as-needed basis, and only when approved by management and security for the purposes of providing support, maintenance, or improving service quality. All of our employees undergo background checks as part of their employment with us.

11. Uptime. Over years of continuous service, we have consistently met or exceeded a 99.9% uptime.

12. Application Security. Our development teams follow the latest security best practices when developing software and automates security testing throughout the development lifecycle whenever possible. The following general security measures have been taken with regard to our applications:

- User sessions will timeout after defined periods of inactivity.
- Session credentials are validated on each page accessed.
- Sensitive data (including user credentials, credit card, etc.) are transmitted between client and server machines using a minimum of TLS 1.2 encryption. (SSL and lower versions of TLS are not supported.)
- Data in transit, such as customer information transmitted to and from our system is handled via secure FTP.
- Sensitive data are stored and handled as encrypted values as necessary to the AES 256 standard.
- Activity logging is performed and monitored.
- Access to our production platforms requires that users provide a username/password combination to access the site and incorporates industry standard password complexity and expiration features which can be configured to conform to our customers' security policies. We also support this use of single sign on (SSO) for customers with this capability.

13. Monitoring System Activities. We monitor system activity with Security Information and Event Management (SIEM) and Cloud Access Security Broker (CASB) systems. Security events and alerts are aggregated to and correlated into a centralized repository.

14. Customer Responsibilities. Customer is responsible for ensuring that administrators' use of and the processing of personal data in our platform is in accordance with best practices for protection of data. The Customer manages the user rights in the platform, including which people are granted administrator rights and which rights each administrator is granted. Customer i) must keep all access credentials current and not share such information with unauthorized parties; ii) shall promptly report to us any suspicious activities related to Customer's account; iii) shall appropriately configure user and role-based access control and iv) otherwise comply with instructions provided by us to Customer.

15. Vulnerability Detection and Management. We regularly conduct penetration tests throughout the year and engages one or more independent third parties to conduct penetration tests of the platform at least annually. We also run weekly vulnerability scans for our platform using updated vulnerability databases. We will provide executive summaries of such testing upon reasonable request. Any vulnerability discovered are prioritized for remediation by us and we will use commercially reasonable efforts to address and remediate vulnerabilities in accordance with our policies in place.

16. Third Party Audits. The hosting facilities utilized by us shall be assessed by independent third-party auditors as described in the following audits and certifications ("**Third-Party Audits**"), on at least an annual basis:

- ISO27001
- SOC 2 Type II

Third-Party Audits are made available to Customer upon reasonable written request. To the extent we decide to discontinue a Third-Party Audit, an alternative audit will be adopted or maintained using an equivalent, industry-recognized framework.