|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| C:\Users\ANDERM\Desktop\HCA-logo.png | Data Share Agreement  [DESCRIPTION] | | | HCA Contract Number:  K | |
| Receiving Party Contract Number: \_\_\_\_\_\_ | |
| This Data Share Agreement (“Agreement” or “DSA”) is made by and between the state of Washington Health Care Authority (“HCA”) and the party whose name appears below (“Receiving Party”) | | | | | |
| Receiving Party Name | | | Receiving Party doing business as (DBA) | | |
|  | | |  | | |
| Receiving Party Address | | | Receiving Party Contact Name, Title (Contract Manager) | | |
|  | | |  | | |
| Receiving Party Contact Telephone | | | Receiving Party Contact Email Address | | |
|  | | |  | | |
| HCA Program | | | HCA Division/Section | | |
|  | | |  | | |
| HCA Contact Name, Title (Contract Manager) | | | HCA Contact Address | | |
|  | | | 626 8th Avenue SE, PO Box 45564  Olympia, WA 98504-5564 | | |
| HCA Contact Telephone | | | HCA Contact Email Address | | |
|  | | |  | | |
| The parties signing below warrant that they have read and understand this Agreement, and have authority to execute this Agreement. This Agreement will be binding on HCA only upon signature by both parties. | | | | | |
| Receiving Party Signature | | Printed Name and Title | | | Date Signed |
|  | |  | | |  |
| HCA Signature | | Printed Name and Title | | | Date Signed |
|  | |  | | |  |

Table of Contents

1. Background (optional) 2

2. Purpose of the DSA 2

3. Justification and Authority for Data Sharing 2

4. Definitions 2

5. Description of Data to be Shared 2

6. Data Classification 2

7. Constraints on Use of Data 2

8. Security of Data 2

9. Data Confidentiality and Non-Disclosure 2

10. Public Disclosure 2

11. Data Shared with Subcontractors 2

12. HIPAA Compliance 2

13. Non PHI Data Breach Notification 2

14. Amendments and Alterations 2

15. Assignment 2

16. Dispute Resolution (Option 1: Vendor/Contractor) 2

17. Dispute Resolution (Option 2: Agencies) 2

18. Entire Agreement 2

19. Governing Law and Venue 2

20. Incorporated Documents and Order of Precedence 2

21. Inspection 2

22. Insurance 2

23. Legal Notices 2

24. Maintenance of Records 2

25. Responsibility 2

26. Severablility 2

27. Survival Clauses 2

28. Term and Termination 2

29. Waiver 2

30. Signatures and Counterparts 2

Schedule 1: Description of Shared Data

Exhibit A: Data Security Requirements

Exhibit B: User Agreement on Non-Disclosure of Confidential Information

# Background

Explain the context for sharing the data – who’s who and how we got here

# Purpose of the DSA

The purpose of this Data Share Agreement (DSA) is to identify, describe and protect the Medicaid data being provided by HCA from ProviderOne to the Receiving Party. The purpose for sharing the Data is for the Receiving Party to      .

# Justification and Authority for Data Sharing

The Data to be shared under this DSA are necessary to comply with

[Explain the justification for the data sharing and provide the statutory or rule authority for the data to be shared.]

# Definitions

**“Agreement”** means this Data Share Agreement.

**“Authorized User”** means an individual or individuals with an authorized business need to access HCA’s Confidential Information under this DSA.

**“Breach”** means the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the Protected Health Information, with the exclusions and exceptions listed in 45 CFR 164.402.

**“Business Associate”** means a Business Associate as defined in 45 CFR 160.103, who performs or assists in the performance of an activity for or on behalf of HCA, a Covered Entity, that involves the use or disclosure of protected health information (PHI). Any reference to Business Associate in this DSA includes Business Associate’s employees, agents, officers, Subcontractors, third party contractors, volunteers, or directors.

**“Business Associate Agreement”** means the HIPAA Compliance section of this DSA (Section 13) and includes the Business Associate provisions required by the U.S. Department of Health and Human Services, Office for Civil Rights.

**“CFR”** means the Code of Federal Regulations. All references in this DSA to CFR chapters or sections will include any successor, amended, or replacement regulation. The CFR may be accessed at <http://www.ecfr.gov/cgi-bin/ECFR?page=browse>

**“Client”** means an individual who is eligible for or receiving Medicaid services.

**“Confidential Information”** means information that is exempt from disclosure to the public or other unauthorized persons under Chapter 42.56 RCW or other federal or state laws. Confidential Information comprises both Category 3 and Category 4 Data as described in Section 6, *Data Classification*, which includes, but is not limited to, Personal Information and Protected Health Information. For purposes of this DSA, Confidential Information means the same as “Data.”

**“Contract Administrator”** means the individual designated to receive legal notices and to administer, amend, or terminate this DSA.

**“Contract Manager”** means the individual identified on the cover page of this DSA who will provide oversight of the activities conducted under this DSA.

**“Covered Entity”** means HCA, which is a Covered Entity as defined in 45 CFR 160.103, in its conduct of covered functions by its health care components.

**“Data”** means the information that is disclosed or exchanged as described by this DSA. For purposes of this DSA, Data means the same as “Confidential Information.”

**“Designated Record Set”** means a group of records maintained by or for a Covered Entity, that is: the medical and billing records about Individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or Used in whole or part by or for the Covered Entity to make decisions about Individuals.

**“Disclosure”** means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

**“DSA”** means this Data Share Agreement.

**“Electronic Protected Health Information (ePHI)”** means Protected Health Information that is transmitted by electronic media or maintained in any medium described in the definition of electronic media at 45 CFR 160.103.

**“HCA”** means the state of Washington Health Care Authority, any section, unit or other entity of HCA, or any of the officers or other officials lawfully representing HCA.

**“HIPAA”** means the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, as amended by the American Recovery and Reinvestment Act of 2009 (“ARRA”), Sec. 13400 – 13424, H.R. 1 (2009) (HITECH Act).

**“HIPAA Rules”** means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Parts 160 and Part 164.

**“Individual(s)”** means the person(s) who is the subject of PHI and includes a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

**“Minimum Necessary”** means the least amount of PHI necessary to accomplish the purpose for which the PHI is needed.

**“Personal Information”** means information identifiable to any person, including, but not limited to, information that relates to a person’s name, health, finances, education, business, use or receipt of governmental services or other activities, addresses, telephone numbers, social security numbers, driver’s license numbers, credit card numbers, any other identifying numbers, and any financial identifiers.

**“Protected Health Information”** or **“PHI”** means information that relates to the provision of health care to an individual; the past, present, or future physical or mental health or condition of an individual; or past, present or future payment for provision of health care to an individual. 45 CFR 160 and 164. PHI includes demographic information that identifies the individual or about which there is reasonable basis to believe, can be used to identify the individual. 45 CFR 160.103. PHI is information transmitted, maintained, or stored in any form or medium. 45 CFR 164.501. PHI does not include education records covered by the Family Educational Right and Privacy Act, as amended, 20 USC 1232g(a)(4)(b)(iv).

**“ProviderOne”** means the Medicaid Management Information System, which is the State’s Medicaid payment system managed by HCA.

**“RCW”** means the Revised Code of Washington. All references in this DSA to RCW chapters or sections will include any successor, amended, or replacement statute. Pertinent RCW chapters can be accessed at: <http://apps.leg.wa.gov/rcw/>.

**“Regulation”** means any federal, state, or local regulation, rule, or ordinance.

**“Receiving Party”** means the entity that is identified on the cover page of this DSA and is a party to this DSA, and includes the entity’s owners, members, officers, directors, partners, trustees, employees, and Subcontractors and their owners, members, officers, directors, partners, trustees, and employees.

**“Security Incident”** means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

**“Subcontract”** means any separate agreement or contract between the Receiving Party and an individual or entity (“Subcontractor”) to perform any duties that give rise to a business requirement to access the Data that is the subject of this DSA.

**“Subcontractor”** means a person or entity that is not in the employment of the Receiving Party, who is performing services or any duties that give rise to a business requirement to access the Data that is the subject of this DSA.

**“USC”** means the United States Code. All references in this DSA to USC chapters or sections will include any successor, amended, or replacement statute. The USC may be accessed at <http://uscode.house.gov/>

**“Use”** includes the sharing, employment, application, utilization, examination, or analysis, of PHI within an entity that maintains such information

**“WAC”** means the Washington Administrative Code. All references in this DSA to WAC chapters or sections will include any successor, amended, or replacement regulation. Pertinent WAC chapters or sections can be accessed at: <http://apps.leg.wa.gov/wac/>.

# Description of Data to be Shared

The Data to be shared is set out in attached Schedule 1: *Description of Shared Data*.

The Data will be provided [how often and how shared – example: one time via an HCA Secure FTP site. HCA will provide access to the Receiving Party.]

# Data Classification

The State classifies data into categories based on the sensitivity of the data pursuant to the Security policy and standards promulgated by the Office of the state of Washington Chief Information Officer. (See Section 4, *Data Security*, of *Securing IT Assets Standards* No. 141.10 in the *State Technology Manual* at <https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets>. Section 4 is hereby incorporated by reference.)

The Data that is the subject of this DSA is classified as indicated below:

Category 1 – Public Information

Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls.

Category 2 – Sensitive Information

Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

Category 3 – Confidential Information

Confidential information is information that is specifically protected from disclosure by law. It may include but is not limited to:

1. Personal Information about individuals, regardless of how that information is obtained;
2. Information concerning employee personnel records;
3. Information regarding IT infrastructure and security of computer and telecommunications systems;

Category 4 – Confidential Information Requiring Special Handling

Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:

1. Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements;
2. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

# Constraints on Use of Data

## The Data being shared/accessed is owned and belongs to HCA.

## This DSA does not constitute a release of the Data for the Receiving Party’s discretionary use. Receiving Party must use the Data received or accessed under this DSA only to carry out the purpose and justification of this agreement as set out in sections 2, Purpose of the Data Sharing, and 3, Justification and Authority for Data Sharing. Any analysis, use, or reporting that is not within the Purpose of this DSA is not permitted without HCA’s prior written consent.

## Any disclosure of Data contrary to this DSA is unauthorized and is subject to penalties identified in law.

# Security of Data

## Data Protection

The Receiving Party must protect and maintain all Confidential Information gained by reason of this DSA against unauthorized use, access, disclosure, modification or loss. This duty requires the Receiving Party to employ reasonable security measures, which include restricting access to the Confidential Information by:

### Allowing access only to staff that have an authorized business requirement to view the Confidential Information.

### Physically securing any computers, documents, or other media containing the Confidential Information.

## Data Security Standards

Receiving Party must comply with the Data Security Requirements set out in Exhibit A and the Washington OCIO Security Standard, 141.10 (<https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets>.) The Security Standard 141.10 is hereby incorporated by reference into this DSA.

## Data Disposition

Upon request by HCA, or at the end of the DSA term, or when no longer needed, Confidential Information/Data must be disposed of as set out in Exhibit A, Section 5 *Data Disposition,* except as required to be maintained for compliance or accounting purposes. Receiving Party will provide written certification of disposition at HCA’s request.

# Data Confidentiality and Non-Disclosure

## Data Confidentiality.

The Receiving Party will not use, publish, transfer, sell, or otherwise disclose any Confidential Information gained by reason of this DSA for any purpose that is not directly connected with the purpose and justification of this DSA, as set out in Sections 1 and 3 above, except: (a) as provided by law; or (b) with the prior written consent of the person or personal representative of the person who is the subject of the Confidential Information.

## Non-Disclosure of Data

The Receiving Party must ensure that all employees or Subcontractors who will have access to the Data described in this DSA (including both employees who will use the Data and IT support staff) are instructed and made aware of the use restrictions and protection requirements of this DSA before gaining access to the Data identified herein. The Receiving Party will also instruct and make any new employee aware of the use restrictions and protection requirements of this DSA before they gain access to the Data.

The Receiving Party will ensure that each employee or Subcontractor who will access the Data signs the *User Agreement on Non-Disclosure of Confidential Information*, Exhibit B hereto. The Receiving Party will retain the signed copy of the *User Agreement on Non-Disclosure of Confidential Information* in each employee’s personnel file for a minimum of six years from the date the employee’s access to the Data ends. The documentation must be available to HCA upon request.

## Penalties for Unauthorized Disclosure of Data

State laws (including RCW 74.04.060 and RCW 70.02.020) and federal regulations (including HIPAA Privacy and Security Rules, 45 CFR Part 160 and Part 164; Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR, Part 2; and Safeguarding Information on Applicants and Beneficiaries, 42 CFR Part 431, Subpart F) prohibit unauthorized access, use, or disclosure of Confidential Information. Violation of these laws may result in criminal or civil penalties or fines.

The Receiving Party accepts full responsibility and liability for any noncompliance by itself, its employees, and its Subcontractors with these laws and any violations of the DSA.

# Public Disclosure

Receiving Party acknowledges that HCA is subject to the Public Records Act (Chapter 42.56 RCW). This DSA will be a “public record” as defined in Chapter 42.56 RCW. Any documents submitted to HCA by Receiving Party may also be construed as “public records” and therefore subject to public disclosure.

# Data Shared with Subcontractors

The Receiving Party will not enter into any Subcontract without the express, written permission of HCA, which will approve or deny the proposed contract in its sole discretion. If Data access is to be provided to a Subcontractor under this DSA, the Receiving Party must include all of the Data security terms, conditions and requirements set forth in this DSA in any such Subcontract. Because the Data includes PHI, Section 13.5 *Subcontracts and Other Third Party Agreements* also applies. In no event will the existence of the Subcontract operate to release or reduce the liability of the Receiving Party to HCA for any breach in the performance of the Receiving Party’s responsibilities.

# HIPAA Compliance

This section of the DSA is the Business Associate Agreement required by HIPAA. The Receiving Party is a “Business Associate” of HCA as defined in the HIPAA Rules.

## **HIPAA Point of Contact.** The point of contact for the Receiving Party for all required HIPAA-related reporting and notification communications from this Section 13 *HIPAA Compliance* and all required Non-PHI Data breach notification communications from Section 14 *Non-PHI* *Data Breach Notification,* is*:*

HCA Privacy Officer

Washington State Health Care Authority

626 8th Avenue SE

PO Box 42700

Olympia, WA 98504-2700

Telephone: 360-725-1116

E-mail: [PrivacyOfficer@hca.wa.gov](mailto:PrivacyOfficer@hca.wa.gov)

## **Compliance**. Business Associate must perform all DSA duties, activities and tasks in compliance with HIPAA, the HIPAA Rules, and all attendant regulations as promulgated by the U.S. Department of Health and Human Services, Office for Civil Rights, as applicable.

## **Use and Disclosure of PHI**. Business Associate is limited to the following permitted and required uses or disclosures of PHI:

### Duty to Protect PHI. Business Associate must protect PHI from, and will use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 (Security Standards for the Protection of Electronic Protected Health Information) with respect to ePHI, to prevent the unauthorized Use or disclosure of PHI for as long as the PHI is within its possession and control, even after the termination or expiration of this DSA.

### Minimum Necessary Standard. Business Associate will apply the HIPAA Minimum Necessary standard to any Use or disclosure of PHI necessary to achieve the purposes of this DSA. See 45 CFR 164.514 (d)(2) through (d)(5).

### Disclosure as Part of the Provision of Services. Business Associate will only Use or disclose PHI as necessary to perform the services specified in this DSA or as required by law, and will not Use or disclose such PHI in any manner that would violate Subpart E of 45 CFR Part 164 (Privacy of Individually Identifiable Health Information) if done by Covered Entity, except for the specific uses and disclosures set forth below.

### Use for Proper Management and Administration. Business Associate may Use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

### Disclosure for Proper Management and Administration. Business Associate may disclose PHI for the proper management and administration of Business Associate, subject to HCA approval, or to carry out the legal responsibilities of the Business Associate, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been Breached.

### Impermissible Use or Disclosure of PHI. Business Associate must report to the contact identified in Subsection 13.1 in writing all Uses or disclosures of PHI not provided for by this DSA within five (5) business days of becoming aware of the unauthorized Use or disclosure of PHI, including Breaches of unsecured PHI as required at 45 CFR 164.410 (Notification by a Business Associate), as well as any Security Incident of which it becomes aware. Upon request by HCA, Business Associate will mitigate, to the extent practicable, any harmful effect resulting from the impermissible Use or disclosure.

### Failure to Cure. If HCA learns of a pattern or practice of the Business Associate that constitutes a violation of the Business Associate’s obligations under the terms of this DSA and reasonable steps by the Business Associate do not end the violation, HCA may terminate this DSA, if feasible. In addition, If Business Associate learns of a pattern or practice of its Subcontractors that constitutes a violation of the Business Associate’s obligations under the terms of their contract and reasonable steps by the Business Associate do not end the violation, Business Associate must terminate the Subcontract, if feasible.

### Termination for Cause. Business Associate authorizes immediate termination of this DSA by HCA, if they determine that Business Associate has violated a material term of this Business Associate Agreement. HCA may, at their sole option, offer Business Associate an opportunity to cure a violation of this Business Associate Agreement before exercising a termination for cause.

### Consent to Audit. Business Associate must give reasonable access to PHI, its internal practices, records, books, documents, electronic data and/or all other business information received from, or created or received by Business Associate on behalf of HCA, to the Secretary of DHHS and/or to HCA for use in determining compliance with HIPAA privacy requirements.

### Obligations of Business Associate Upon Expiration or Termination. Upon expiration or termination of this DSA for any reason, with respect to PHI received from HCA, or created, maintained, or received by Business Associate, or any Subcontractors, on behalf of HCA, Business Associate must:

#### Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

#### Return to HCA or destroy the remaining PHI that the Business Associate or any Subcontractors still maintain in any form;

#### Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 (Security Standards for the Protection of Electronic Protected Health Information) with respect to Electronic Protected Health Information to prevent Use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate or any Subcontractors retain the PHI;

#### Not Use or disclose the PHI retained by Business Associate or any Subcontractors other than for the purposes for which such PHI was retained and subject to the same conditions set out in Subsection 13.3 *Use and Disclosure of PHI* that applied prior to termination; and

#### Return to HCA or destroy the PHI retained by Business Associate, or any Subcontractors, when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

### Survival. The obligations of the Business Associate under this section will survive the termination or expiration of this DSA.

## Individual Rights.

### Accounting of Disclosures.

#### Business Associate will document all disclosures, except those disclosures that are exempt under 45 CFR 164.528, of PHI and information related to such disclosures.

#### Within ten (10) business days of a request from HCA, Business Associate will make available to HCA the information in Business Associate’s possession that is necessary for HCA to respond in a timely manner to a request for an accounting of disclosures of PHI by the Business Associate. See 45 CFR 164.504(e)(2)(ii)(G) and 164.528(b)(1).

#### At the request of HCA or in response to a request made directly to the Business Associate by an Individual, Business Associate will respond, in a timely manner and in accordance with HIPAA and the HIPAA Rules, to requests by Individuals for an accounting of disclosures of PHI.

#### Business Associate record keeping procedures will be sufficient to respond to a request for an accounting under this section for the six (6) years prior to the date on which the accounting was requested.

### Access

#### Business Associate will make available PHI that it holds that is part of a Designated Record Set when requested by HCA or the Individual as necessary to satisfy HCA’s obligations under 45 CFR 164.524 (Access of Individuals to Protected Health Information).

#### When the request is made by the Individual to the Business Associate or if HCA ask the Business Associate to respond to a request, the Business Associate must comply with requirements in 45 CFR 164.524 (Access of Individuals to Protected Health Information) on form, time and manner of access. When the request is made by HCA, the Business Associate will provide the records to HCA within ten (10) business days.

### Amendment.

#### If HCA amends, in whole or in part, a record or PHI contained in an Individual’s Designated Record Set and HCA has previously provided the PHI or record that is the subject of the amendment to Business Associate, then HCA will inform Business Associate of the amendment pursuant to 45 CFR 164.526(c)(3) (Amendment of Protected Health Information).

#### Business Associate will make any amendments to PHI in a Designated Record Set as directed by HCA or as necessary to satisfy HCA’s obligations under 45 CFR 164.526 (Amendment of Protected Health Information).

## **Subcontracts and other Third Party Agreements**. In accordance with 45 CFR 164.502(e)(1)(ii), 164.504(e)(1)(i), and 164.308(b)(2), Business Associate must ensure that any agents, Subcontractors, independent contractors or other third parties that create, receive, maintain, or transmit PHI on Business Associate’s behalf, enter into a written contract that contains the same terms, restrictions, requirements, and conditions as the HIPAA compliance provisions in this Contract with respect to such PHI. The same provisions must also be included in any contracts by a Business Associate’s Subcontractor with its own business associates as required by 45 CFR 164.314(a)(2)(b) and 164.504(e)(5).

## **Obligations**. To the extent the Business Associate is to carry out one or more of HCA’s obligation(s) under Subpart E of 45 CFR Part 164 (Privacy of Individually Identifiable Health Information), Business Associate must comply with all requirements that would apply to HCA in the performance of such obligation(s).

## **Liability**. Within ten (10) business days, Business Associate must notify the contact identified in Subsection 13.1 of any complaint, enforcement or compliance action initiated by the Office for Civil Rights based on an allegation of violation of the HIPAA Rules and must inform HCA of the outcome of that action. Business Associate bears all responsibility for any penalties, fines or sanctions imposed against the Business Associate for violations of the HIPAA Rules and for any imposed against its Subcontractors or agents for which it is found liable.

## Breach Notification.

### In the event of a Breach of unsecured PHI or disclosure that compromises the privacy or security of PHI obtained from HCA or involving HCA clients, Business Associate will take all measures required by state or federal law.

### Business Associate will notify the contact identified in Subsection 13.1 by telephone and in writing within five (5) business days of any acquisition, access, use or disclosure of PHI not allowed by the provisions of this DSA or not authorized by HIPAA Rules or required by law that potentially compromises the security or privacy of the Protected Health Information.

### Business Associate will notify the HCA Privacy Officer identified in Section 13.1 above by telephone or e-mail within five (5) business days of any potential Breach of security or privacy of PHI by the Business Associate or its Subcontractors or agents. Business Associate will follow telephone or e-mail notification with a written (fax or email acceptable) explanation of the Breach, to include the following: date and time of the Breach, date Breach was discovered, location and nature of the PHI, type of Breach, origination and destination of PHI, Business Associate unit and personnel associated with the Breach, detailed description of the Breach, anticipated mitigation steps, and the name, address, telephone number, fax number, and e-mail of the individual who is responsible as the primary point of contact. Business Associate will notify HCA prior to dissemination of any public announcement of a data security Breach involving HCA’s data and include in any such required notifications, the planned date for the public announcement.

### Solely for purposes of the performance of the Proof of Concept as more particularly set forth in Schedule 1 hereto and Schedules A hereto, if a Breach of unsecured PHI is the sole fault of Business Associate then as between Business Associate and HCA, Business Associate will remain liable for claims that may arise from such Breach, including, but not limited to, costs for litigation (including reasonable attorneys’ fees), and reimbursement sought by individuals, including but not limited to, costs for credit monitoring or allegations of loss in connection with the Breach, and to the extent that any claims are brought against HCA, must indemnify HCA from such claims (if such claims arise through no fault or breach by HCA) and Business Associate will be responsible for any other legal or regulatory obligations which may arise under applicable law in connection with such a Breach and will bear all costs associated with complying with legal and regulatory obligations in connection therewith. For avoidance of doubt, “fault” refers to the party’s failure through act or omission to use reasonable procedures to avoid unauthorized access, use or disclosure of Personal Information.

### In the event the Breach is the sole fault of HCA, then as between Business Associate and HCA, HCA will remain liable for claims that may arise from such Breach, including, but not limited to, costs for litigation (including reasonable attorneys’ fees), and reimbursement sought by individuals, including but not limited to, costs for credit monitoring or allegations of loss in connection with the Breach, and to the extent that any claims are brought against Business Associate, will indemnify Business Associate from such claims (if such claims arise through no fault or breach by Business Associate ) and HCA will be responsible for any other legal or regulatory obligations which may arise under applicable law in connection with such a Breach and will bear all costs associated with complying with legal and regulatory obligations in connection therewith. For avoidance of doubt, “fault” refers to the party’s failure, through act or omission, to use reasonable procedures to prevent unauthorized acquisition of, access to or use of such Personal Information.

## Miscellaneous Provisions.

### Regulatory References. A reference in this DSA to a section in the HIPAA Rules means the section as in effect or amended.

### Interpretation. Any ambiguity in this DSA will be interpreted to permit compliance with the HIPAA Rules.

# Non PHI Data Breach Notification

The Breach of non-PHI Data shared under this DSA must be reported to the HCA Privacy Officer at [PrivacyOfficer@hca.wa.gov](mailto:PrivacyOfficer@hca.wa.gov) within five (5) business days of discovery. The Receiving Party must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by applicable law or reasonably requested by HCA in order to meet its regulatory obligations.

# Assignment

The Receiving Party will not assign rights or obligations derived from this DSA to a third party without the prior, written consent of HCA and the written assumption of the Receiving Party’s obligations by the third party.

# Dispute Resolution

## The parties will use their best, good faith efforts to cooperatively resolve disputes and problems that arise in connection with this DSA. Both parties will continue without delay to carry out their respective responsibilities under this DSA while attempting to resolve any dispute. When a genuine dispute arises between HCA and the Receiving Party regarding the terms of this DSA or the responsibilities imposed herein and it cannot be resolved between the parties’ Contract Managers, either party may initiate the following dispute resolution process.

## The initiating party will reduce its description of the dispute to writing and deliver it to the responding party (email acceptable). The responding party will respond in writing within five (5) Business Days (email acceptable). If after five (5) additional Business Days the parties have not resolved the Dispute, it will be submitted to the HCA Director, who may employ whatever dispute resolution methods the Director deems appropriate to resolve the dispute.

## A party's request for a dispute resolution must:

### Be in writing;

### Include a written description of the dispute;

### State the relative positions of the parties and the remedy sought;

### State the Contract Number and the names and contact information for the parties;

## This dispute resolution process constitutes the sole administrative remedy available under this DSA. There is no right under this DSA to an adjudicative proceeding under the Administrative Procedure Act.

# Entire Agreement

This DSA, including all documents attached to or incorporated by reference, contains all the terms and conditions agreed upon by the parties. No other understandings or representations, oral or otherwise, regarding the subject matter of this DSA, will be deemed to exist or bind the parties.

# Incorporated Documents and Order of Precedence

## Each of the documents listed below is, by this reference, incorporated into this DSA as though fully set forth herein.

### Schedule 1 – Description of Shared Data.

### Exhibit A – Data Security Requirements.

### Exhibit B – User Agreement on Non-Disclosure of Confidential Information.

### Section 4 of OCIO 141.10, *Securing Information Technology Assets Standards: Data Security* (<https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets>.)

## In the event of any inconsistency in this DSA, the inconsistency will be resolved in the following order of precedence:

### Applicable federal and state statutes, laws, and regulations;

### Sections of this DSA;

### Attachments, Exhibits and Schedules to this DSA.

# Inspection

No more than once per quarter during the term of this DSA and for ten (10) years following termination or expiration of this DSA, HCA will have the right at reasonable times and upon no less than five (5) business days prior written notice to access the Receiving Party’s records and place of business for the purpose of auditing, and evaluating the Receiving Party’s compliance with this DSA and applicable laws and regulations.

# Insurance

## HCA certifies that it is self-insured under the State’s self-insurance liability program, as provided by RCW 4.92.130, and will pay for losses for which HCA is found liable.

## The Receiving Party certifies that it is self-insured, is a member of a risk pool, or maintains the types and amounts of insurance identified below and will provide certificates of insurance to that effect to HCA upon request.

## Required Insurance or Self-Insured Equivalent

### Commercial General Liability Insurance (CGL) covering the risks of bodily injury (including death), property damage, and contractual liability, with a limit of not less than $1 million per occurrence, $2 million aggregate.

### Cyber Liability/Privacy Breach Response Coverage. For the term of this DSA and 3 years following its termination or expiration, Receiving Party must maintain insurance to cover costs incurred in connection with a security incident, privacy Breach, or potential compromise of Data, including:

#### Computer forensics assistance to assess the impact of a Data Breach, determine root cause, and help determine whether and the extent to which notification must be provided to comply with Breach notification laws;

#### Notification and call center services for individuals affected by a security incident, or privacy Breach;

#### Breach resolution and mitigation services for individuals affected by a security incident or privacy Breach, including fraud prevention, credit monitoring, and identity theft assistance; and

#### Regulatory defense, fines, and penalties from any claim in the form of a regulatory proceeding resulting from a violation of any applicable privacy or security law(s) or regulation(s).

### If any of the required policies provide coverage on a claims-made basis:

#### The retroactive date must be shown and must be before the date of the DSA or of the beginning of DSA work.

#### If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a retroactive date prior to the DSA effective date, the Receiving Party must purchase “extended reporting” coverage for a minimum of 3 years after completion of DSA work.

The State of Washington, including but not limited to HCA, must be named as additional insureds.

In the event of cancellation, non-renewal, revocation or other termination of any insurance coverage required by this DSA, Receiving Party must provide written notice of such to HCA within one (1) Business Day of Receiving Party’s receipt of such notice.

By requiring insurance herein, HCA does not represent that coverage and limits will be adequate to protect Receiving Party. Such coverage and limits will not limit Receiving Party’s liability under the indemnities and reimbursements granted to HCA in this DSA.

Schedule 1: Description of Shared Data

|  |  |  |
| --- | --- | --- |
| User Agreement on Non-Disclosure of Confidential Information | | |
| Your organization has entered into a Data Share Agreement with the state of Washington Health Care Authority (HCA) that will allow you access to data and records that are deemed Confidential Information as defined below. Prior to accessing this Confidential Information you must sign this *User Agreement on Non-Disclosure of Confidential Information.* | | |
| Confidential Information | | |
| “Confidential Information” means information that is exempt from disclosure to the public or other unauthorized persons under Chapter 42.56 RCW or other federal or state laws. Confidential Information includes, but is not limited to, Protected Health Information and Personal Information. For purposes of the pertinent Data Share Agreement, Confidential Information means the same as “Data.”  “Protected Health Information” means information that relates to: the provision of health care to an individual; the past, present, or future physical or mental health or condition of an individual; or the past, present or future payment for provision of health care to an individual and includes demographic information that identifies the individual or can be used to identify the individual.  “Personal Information” means information identifiable to any person, including, but not limited to, information that relates to a person’s name, health, finances, education, business, use or receipt of governmental services or other activities, addresses, telephone numbers, social security numbers, driver license numbers, credit card numbers, any other identifying numbers, and any financial identifiers. | | |
| Regulatory Requirements and Penalties | | |
| State laws (including, but not limited to, RCW 74.04.060, RCW 74.34.095, and RCW 70.02.020) and federal regulations (including, but not limited to, HIPAA Privacy and Security Rules, 45 CFR Part 160 and Part 164; Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR, Part 2; and Safeguarding Information on Applicants and Beneficiaries, 42 CFR Part 431, Subpart F) prohibit unauthorized access, use, or disclosure of Confidential Information. Violation of these laws may result in criminal or civil penalties or fines. | | |
| User Assurance of Confidentiality | | |
| In consideration for HCA granting me access to the Confidential Information that is the subject of this Agreement, I agree that I:   1. Will access, use, and disclose Confidential Information only in accordance with the terms of this Agreement and consistent with applicable statutes, regulations, and policies. 2. Have an authorized business requirement to access and use the Confidential Information. 3. Will not use or disclose any Confidential Information gained by reason of this Agreement for any commercial or personal purpose, or any other purpose that is not directly connected with this Agreement. 4. Will not use my access to look up or view information about family members, friends, the relatives or friends of other employees, or any persons who are not directly related to my assigned job duties. 5. Will not discuss Confidential Information in public spaces in a manner in which unauthorized individuals could overhear and will not discuss Confidential Information with unauthorized individuals, including spouses, domestic partners, family members, or friends. 6. Will protect all Confidential Information against unauthorized use, access, disclosure, or loss by employing reasonable security measures, including physically securing any computers, documents, or other media containing Confidential Information and viewing Confidential Information only on secure workstations in non-public areas. 7. Will not make copies of Confidential Information, or print system screens unless necessary to perform my assigned job duties and will not transfer any Confidential Information to a portable electronic device or medium, or remove Confidential Information on a portable device or medium from facility premises, unless the information is encrypted and I have obtained prior permission from my supervisor. 8. Will access, use or disclose only the “minimum necessary” Confidential Information required to perform my assigned job duties. 9. Will not distribute, transfer, or otherwise share any software with anyone. 10. Will forward any requests that I may receive to disclose Confidential Information to my supervisor for resolution and will immediately inform my supervisor of any actual or potential security breaches involving Confidential Information, or of any access to or use of Confidential Information by unauthorized users. 11. Understand at any time, HCA may audit, investigate, monitor, access, and disclose information about my use of the Confidential Information and that my intentional or unintentional violation of the terms of this Agreement may result in revocation of privileges to access the Confidential Information, disciplinary actions against me, or possible civil or criminal penalties or fines. 12. Understand that my assurance of confidentiality and these requirements will continue and do not cease at the time I terminate my relationship with my employer. | | |
| Signature | | |
| Print User’s Name | User Signature | Date |
|  |  |  |