SEDERA, INC. PRIVACY POLICY AND PROCEDURES

1. PURPOSE. The purpose of this Policy is to:

   1.1. Outline and document the compliance processes for use of information and documents within Sedera Health ("Sedera") operations. Compliance is necessary because Sedera's operations necessarily involve private information regarding Employee Members ("Members"). Member information includes both personal identifying information and sensitive personal information regarding Members' health.

   1.2. Various privacy rules, standards, and regulations offer multiple titles and acronyms for this information. The standards vary across all fifty states and the federal government. Sedera seeks to provide a baseline for information security through this policy. For purposes of Sedera's policy, both personal identifying information and sensitive personal information regarding Members' Health Care Sharing will be called "Sensitive Information," and the goal of this policy is to prevent any unauthorized disclosure of any Sensitive Information.

   1.3. Sensitive Information means:

      1.3.1. Information that alone or in conjunction with other information identifies an individual, including an individual's:

      - Name, social security number, date of birth, or government-issued identification number; address, unique Member identification number,
      - bank account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to a Member's financial account;
      - information that identifies a Member and relates to:
      - the physical or mental health or condition of the Member
      - the provision of health care to the Member; or
      - payment for sharing of medical expenses to the Member.

   1.4. Sensitive Information does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government.

   1.5. Healthcare Sharing (HCS) means a community of individuals who are committed to sharing each other's healthcare related expenses.

   1.6. Sedera Health maintains company client information that may be subject to disclosure by state or federal law.

   1.7. This policy is proper for public dissemination, and it also provides a reference for internal compliance and training.

2. SCOPE. This Policy represents the efforts performed to ensure confidentiality of Sensitive Information is maintained. All employees who have access to Sensitive Information must be trained in and comply with this Policy. For the purposes of this policy, the following terms are defined:

3. GENERAL POLICIES.

   3.1. No Waiver of Privacy Rights. No Member will be required to waive any privacy rights under the Privacy Rule as a condition of participating in the Sedera HCS model. Privacy rights waivers are not enforceable and will not be accepted.

   3.2. Privacy/Security Officer and Contact Person. This Officer will be responsible for the development and implementation of policies and procedures relating to privacy and security, including but not limited to this Privacy Policy. This Officer or appropriate designee will also serve as the contact person for Members who have questions, concerns, or any complaints regarding Sensitive Information.

   3.3. Initial Workforce Training. All employees who have access to Sensitive Information will be trained on these policies and procedures. Training sessions will be held to achieve the goal that all employees will be instructed regarding the need to protect unauthorized disclosure of Sensitive Information prior to first access to Sensitive Information, and will be formally trained within 30 days of the date of first access to Sensitive Information. Each employee will be required to acknowledge that they have been trained on and will comply with this Policy. The record of training will be maintained by the Privacy Officer or his/her designee.

   3.4. Annual Workforce Training. All employees who have access to Sensitive Information will have annual update training on changes to these policies and procedures. The record of training will be maintained by the Privacy Officer or his/her designee.

   3.5. Training Records. Sedera employees shall indicate receipt of training on Sensitive Information by electronic or physical signature. Such evidence of training on Sensitive Information shall be maintained, both initial workforce training and annual workforce training, for a period of six years from the date of training.

   3.6. Sanctions for Violations of Privacy Policy. Sanctions for using or disclosing Sensitive Information in violation of this Policy will be imposed in accordance with applicable discipline policy, up to and including termination.

   3.7. Prohibition on Sale of Sensitive Information. There is no selling Sensitive Information in any manner for any purpose, including the sale or exchange of Sensitive Information for any form of trade or compensation. All employees are strictly prohibited from arranging for or providing any Sensitive Information for sale, for any purpose whatsoever.

4. MEMBER PRIVACY RIGHTS UNDER THIS POLICY. The Privacy Officer will respond to Member requests as follows:

4.1. Right to Inspect and Copy Sensitive Information. When Sedera receives a written request from the Member, Sedera, through its Privacy Officer, will make electronic records of Sensitive Information available within fifteen (15) days, and written records within thirty (30) days. If a written copy is requested, a reasonable fee for the costs of copying, mailing, or other supplies associated with the request will be charged. The request may be denied in certain limited circumstances related to the wellbeing of the Member. If you are denied access to your Sensitive Information, you may request that the denial be reviewed by submitting a written request to the Privacy Officer identified below.[1]

4.2. Amendment of Sensitive Information. The Privacy Officer will make reasonable amendments to Sensitive Information when the Sensitive Information is created or maintained by Sedera or a Service Provider. The Privacy Officer will communicate any approval or denial of an amendment of Sensitive Information maintained by the Privacy Officer or a Service Provider to the Member. An example of an unreasonable request would be for the Privacy Officer to alter a medical record received; in such case the Member would be advised to ask the medical provider who created the record for such amendment.

4.3. Accounting of Disclosures. The Privacy Officer will make available to the Member the information required to provide an accounting of disclosures. The Privacy Officer will prepare and deliver any such accounting requested. The accounting will not include (1) disclosures for purposes of Sedera's health sharing operations; (2) disclosures made to a Member; (3) disclosures made pursuant to a Member's authorization; (4) disclosures made to friends or family in a Member's presence or because of an emergency; (5) disclosures for permissible law enforcement purposes; and (6) disclosures incidental to otherwise permissible disclosures. To request this list or accounting of disclosures, the Member must submit a request in writing to the Privacy Officer. A Member's request must state the period the accounting covers, which may not be longer than six years before the date of the request. A Member's request should indicate in what form a Member wants the list (for example, paper or electronic). The first list a Member requests within a 12-month period will be provided free of charge. For additional lists, the Privacy Officer will notify a Member of the cost involved and a Member may choose to withdraw or modify the request at that time before any costs are incurred.

4.4. The Right to Restrict the Use and Request Confidential Communications. A Member has the right to request a restriction of uses and disclosures of their Sensitive Information. A Member also has the right to restrict communication of their Sensitive Information if the Member informs the Privacy Officer that communicating the information may endanger the Member. Requests will be deemed unreasonable if they limit the access and use that is necessary for HCS facilitation. If the Privacy Officer agrees to the request for a restriction, the Privacy Officer will not use or disclose the Sensitive Information in violation of the restriction, except when needed for emergency treatment, at the written request of the Member (by authorization), or when the use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of

[1] No charge shall be required for requests from California members.

such law. The Privacy Officer may terminate its agreement to a restriction, if the Member agrees to or requests the termination in writing; or, the Privacy Officer informs the Member that it is terminating its agreement to a restriction. The termination is only effective with respect to Sensitive Information created or received after the Member is informed.

4.5. Requests for Alternative Communication Means or Locations. Members may request to receive communications regarding their Sensitive Information by alternative means or at alternative locations. For example, Members may ask to be called only at work rather than at home. These requests will be honored if, in the sole discretion of the Privacy Officer, the requests are reasonable. However, the Privacy Officer will accommodate such a request if the Member clearly provides information that the disclosure of all or part of that information could endanger the Member. All such requests should be forwarded to the Privacy Officer when received.

4.6. Right to receive a copy of this Policy. A copy of this policy will be posted on the Sedera website, on a page titled "Your Privacy Rights," so that Members will have an explanation of:

- the uses and disclosures of Sensitive Information
- the individual's privacy rights, and
- Sedera's policies and procedures with respect to the Sensitive Information.

5. COMPLAINT PROCEDURES.

5.1. Complaints. A Member can file a complaint regarding the Privacy Rule or any matter described in this Privacy Policy with the Privacy Officer by sending a written description of the facts and circumstances and the acts that are the subject of the complaint to:

Attn: Privacy Officer
Sedera, Inc.
5113 Southwest Parkway, Ste. 175
Austin, TX 78735

All complaints will be forwarded to the Privacy Officer. The Privacy Officer is responsible for any response and taking necessary actions to change this complaint process or this Privacy Policy. No response from the Privacy Officer is required. A copy of this complaint procedure will be provided to the Member upon request. No employee will intimidate, threaten, coerce, discriminate against, or take other retaliatory action against Members for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under the Privacy Policy or any federal, state, or local law or rule.

6. DOCUMENTATION. The Privacy Officer will ensure that privacy files are maintained for a period of 6 years from the date of the event as described below, or when appropriate for 6

years after the end of the Membership Year in which the document was created. Sedera will destroy Sensitive Information that is older than 6 years on a calendar basis.

6.1. Training. A copy of training materials is maintained along with a log of all employees present at the training. This documentation is maintained for a period of 6 years.

6.2. Disclosures. Authorized disclosures per this policy under specific authorizations and to individuals will be documented and maintained for a period of 6 years. Sedera will not document disclosures of Sensitive Information as defined above, or routine Disclosures of minimum necessary data to a vendor or other entity with which Sedera necessarily must use for the purposes of HCS.

6.3. Complaints. Any complaint made regarding this Policy, any response, and actions taken to resolve the complaint, if any, will be maintained for a period of 6 years.

6.4. Inadvertent Disclosure of Sensitive Information. The Privacy Officer will document any unauthorized disclosure of Sensitive Information. All incidents need to be reviewed by the Privacy Officer to determine whether this constitutes a Breach of insecure Sensitive Information. Any questions should be referred to the Privacy Officer.

6.5. Security Incidents. See the Incident Policy below.

6.6. Privacy Notice Distribution. A copy of the Privacy Notice will be posted on the company website. Copies by Members will be sent as requested. The first hard copy will be sent at no charge. Subsequent copies will be mailed for a reasonable cost. The Privacy Officer will notify a Member of the cost involved and a Member may choose to withdraw the request at that time before any costs are incurred.

6.7. Requests for Member Rights. Written requests for Privacy Notice rights, the written response if any, and the resolution of the request will be retained in the Member's file for a period of 6 years.

7. VENDORS. Members expressly authorize Sedera to have access to and maintain Sensitive Information. Because Sedera Health's policy forms a floor of information security, it is important that the vendors with whom Sedera engages in health care sharing maintain at a minimum the same level of information security. The following policy covers the relationship with those vendors.

7.1. Secure Vendors. A Secure Vendor is an entity or person who: 1) Performs or assists in performing a HCS function or activity involving the use and disclosure of Sensitive Information (including needs processing or administration; data analysis, etc.); or 2) Provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the Service Provider access to Sensitive Information. A Secure Vendor, if not already authorized by the Member through another privacy relationship with the vendor, is required to enter an agreement with Sedera that it will comply with the standards of this policy, or a similar policy, such as a HIPAA Business Associate

Agreement, as a baseline requirement. Secure Vendors will only use and disclose Sensitive Information consistent with this Policy.

7.2. Contracts with Secure Vendors. Sedera may disclose Sensitive Information to a Secure Vendor and allow the Secure Vendor to create or receive Sensitive Information on its behalf. However, prior to doing so, the Sedera must first obtain written assurances from the Secure Vendor that it will appropriately safeguard the information. This assurance is in the form of a Secure Vendor Contract, or a similar contract such as a HIPAA Business Associate Agreement. As Sedera is not required to fall under HIPAA, any signature of Sedera upon a HIPAA Business Associate Agreement merely reflects the agreement to safeguard Sensitive Information of Sedera Members.

8. DISCLOSURES.

8.1. No Disclosure of Sensitive Information for Non-Health HCS Purposes. Sensitive Information may not be used or disclosed for any purpose except as defined and limited in this Policy. Sensitive Information may not be used or disclosed for the payment or operations of "non-health" benefits (e.g., disability, worker's compensation, life insurance, etc.), unless the Member has provided an authorization.
IMPORTANT NOTE: All transmissions of Sensitive Information are sent or received in a secure environment. The level of security will depend on the nature of the data. Member "Needs" information is sent via encrypted email. Disclosure can be made to anyone designated as a personal representative, or attorney-in-fact by the Member. The Member must provide a written notice/authorization and supporting documents such as a power of attorney. Sedera will not disclose information to a personal representative if there is a reasonable belief that the Member has been, or may be, subjected to domestic violence, abuse, or neglect by such person; or treating such person as a personal representative could endanger the Member.

8.2. Breadth of Disclosures. Sensitive Information disclosures are limited to the "Minimum Necessary" data to accomplish the purpose for the disclosure. This "minimum necessary" standard does not apply to the following:

- uses or disclosures made to the Member upon request;
- uses or disclosures made pursuant to a valid authorization; or,
- disclosures required by law or regulation made pursuant to a valid subpoena or request from a governmental entity.

Minimum Necessary is further defined for enrollment purposes as the name, HCS elections, effective and termination of coverage dates, demographics required to identify the individual, and balance data for account balance purposes.

8.3. Routine Disclosures. Routine disclosures to insurers, Third Party Administrators, employers, and Service Providers for the purpose of HCS administration can be made without prior Member authorization. The transmissions will comply with the Minimum

Necessary Rule and be limited to enrollment/disenrollment data and monetary account balance information for the purpose of making enrollment changes.

8.4. Other Routine Disclosures. Information regarding client companies is governed with a "cooperative consent" model of disclosure. In the business context, Sedera serves client companies. The Services Agreement that is between Sedera Health and a client company executive may be subject to disclosure under state or federal law. If such disclosure is requested, both Sedera and client companies retain privacy rights and individual can decide whether such disclosure is lawful and/or appropriate. If Sedera decides to disclose any information regarding a client company, a client company executive will be contacted prior to disclosure to facilitate discussion and permit the client company to object and/or take any action, legal or otherwise, it believes is required given the situation. If both Sedera and the respective client company are in agreement to disclose, disclosure will occur and the client company will receive notice of any documents or information disclosed.

8.5. Disclosures of Summary Health Information. Summary health information may be disclosed without prior Member authorization. This information does not provide a reasonable basis to believe that it can be used to identify an individual. Summary health information must have the following 18 identifiers redacted:

- names;
- geographic subdivisions smaller than a state, aggregated to the level of a five-digit ZIP code;
- dates (except year) directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age (ages and elements may be aggregated into a single category of age 90 or older);
- telephone numbers;
- fax numbers;
- e-mail addresses;
- Social Security numbers;
- medical record numbers;
- HCS beneficiary numbers;
- account numbers;
- certificate/license numbers;
- vehicle identifiers and serial numbers, including license plate numbers;
- device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) addresses;
- biometric identifiers, including finger and voice prints;
- full face photographic images and any comparable images; and
- any other unique identifying number or characteristic.

Disclosures of summary health information must be pre-approved by the Privacy Officer.

8.6. Privacy Certification. For Sedera to release any Sensitive Information to the client employer other than the Minimum Necessary information defined above, the client employer must be permitted by the Member to receive such information, certify that their Service Agreement has been amended to comply with the Privacy Policy and that they agree to comply. The client employer must certify to:

- Not to use or further disclose Sensitive Information other than as permitted or required by HCS, or as required by law,
- Ensure that any subcontractors or vendors agree to the same restrictions,
- Not use or disclose Sensitive Information for employment related actions,
- Report to the HCS any use or disclosure that is inconsistent with this Privacy Policy,
- Make the Sensitive Information accessible to the Members,
- Allow Members to amend their Sensitive Information,
- Provide an accounting of its disclosures of Sensitive Information as required by this Privacy Policy,
- Return and destroy all Sensitive Information when no longer needed, if feasible, and
- Establish adequate firewalls.

8.7. Disclosures Pursuant to an Authorization. Sensitive Information may be disclosed by Member authorization as directed by the Member. Any issue related to a disclosure and the wellbeing of the Member, or another person named in the Sensitive Information, should be brought to the Privacy Officer prior to making the disclosure. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization. An Authorization is a separate form that must have a note that it can be revoked at any time, identify the person who is the subject of the Sensitive Information, identify the person(s) that can receive the Sensitive Information, the purpose of the request, have an expiration date, and a statement that Sedera will not condition sharing of needs based on the signing of the authorization.

9. UNAUTHORIZED DISCLOSURE RESPONSE POLICY (NON-BREACH).

9.1. Scope and Purpose. This Unauthorized Disclosure Response Policy describes actions taken regarding an unauthorized disclosure of Sensitive Information, a disclosure that does not otherwise comply with the Disclosure Section of this Policy provided above, either by an employee of Sedera or a Secure Vendor. Member notices are not required unless it is determined that the disclosure constitutes a Breach as determined below.

9.2. Reporting to Privacy Officer. All such unauthorized disclosures will be reported as soon as reasonably possible to the Privacy Officer. Each employee reporting an unauthorized disclosure will also report the event to their Director/Manager.

9.3. Mitigation. The Privacy Officer will seek to mitigate, to the extent possible, any harmful effects for an unauthorized disclosure. The Privacy Officer will inquire that the unauthorized recipient of the Sensitive Information confirms that they have immediately

destroyed the data without further disclosure. Email or other confirmation will be retained as part of the Incident Documentation. Mitigation may include additional options as determined by the Privacy Officer such as ID Theft monitoring services.

10. BREACH DETERMINATION. A "Breach" under this policy is an unauthorized transmission of unsecure Sensitive Information. The Privacy Officer will review the facts and circumstances to make the Breach determination. This will include a two-step analysis as described below:

    10.1. Step One: Determine whether the three exclusions below apply. The following unauthorized disclosures are not a Breach:

    - Any unintentional acquisition, access, or use of Sensitive Information, if it was made in good faith and within the scope of authority and does not result in further use or disclosure.
    - Any inadvertent disclosure to a person authorized to access Sensitive Information at the same covered entity or secure vendor, or to an entity which has a business relationship with Sedera and who, within its normal business operations, has a privacy policy utilizing federal and state standards to protect Sensitive Information, and the information received as a result of such disclosure is not further used or disclosed.
    - A disclosure of Sensitive Information where Sedera or a secure vendor has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

    10.2. Step Two: If an unauthorized disclosure does not fit one of the exclusions above, then the unauthorized disclosure is presumed to be a Breach unless it can be demonstrated that there is a low probability that the Sensitive Information has been compromised based on a risk assessment of at least the following factors:

    - The nature and extent of the Sensitive Information involved, including the types of identifiers and the likelihood of re-identification;
    - The unauthorized person who used the Sensitive Information or to whom the disclosure was made;
    - Whether the Sensitive Information was actually acquired or viewed; and
    - The extent to which the risk to the Sensitive Information has been mitigated.

11. BREACH NOTICES. When the Privacy Officer determines that an unauthorized disclosure of Sensitive Information is a Breach, then notices must be sent to the Members whose Sensitive Information was compromised. The Notice will include the facts related to the disclosure and the mitigation that has been completed.

    11.1. Non-Breach Notices. When the Privacy Officer determines that the unauthorized disclosure is not a Breach there is no notice sent to the Members.

11.2. Breach Notices. When the Privacy Officer determines that the unauthorized disclosure is a Breach, a notice will be provided to the Members without undue delay, and in no case longer than 30 days. A Breach shall be treated as discovered as of the first day on which such Breach is known, or, by exercising reasonable diligence would have been known. Knowledge of a Breach exists when the Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is a workforce employee or agent. The Privacy Officer will communicate the facts and circumstances that caused the Breach, the mitigation effort and response, the number of Members that were affected and the data that was disclosed. The notice will include:

- Description of the Event
- Date of Event (if known)
- Date of the Discovery
- Number of individuals affected
- The types of unsecured Sensitive Information that were involved (such as the name, Social Security Number, date of birth, home address, account number or disability code of the affected individuals)
- If involving a Secure Vendor(s), a description of the steps the Secure Vendor(s) is/are taking to investigate, mitigate losses related to and protect against any further disclosures or Breaches
- Contact information for any affected individuals to ask questions or learn additional information: Name and Title, Address, E-mail address, and Telephone Number
- The Notice will be titled "Notice of Data Breach," and will present the information under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information" in at least 10 pt. font. Additional information may be provided as a supplement to the notice.

11.3. Documentation. The Privacy Officer will maintain a file of each unauthorized disclosure that is made that is not in compliance with this Privacy Policy as soon as there is an awareness of the disclosure. The record will contain a description of the Sensitive Information disclosed, to whom it was disclosed, when the Member was notified of the disclosure, an explanation of any action taken to mitigate the damages that the disclosure created, and a description of any action that was taken regarding the error.

11.4. Public Notice. Notice will be provided to prominent media outlets serving a state or jurisdiction following the discovery of a Breach if unsecured Sensitive Information of more than 500 residents of such state or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such Breach.

12. SECURITY INCIDENT RESPONSE PLAN AND PROCEDURES. This Incident Response Procedure is in place to ensure incidents related to the areas and systems that maintain Sensitive Information are detected, responded to appropriately and action is taken to prevent future incidents. Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to:

- Theft, damage, or unauthorized access (e.g., unauthorized logins, papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry)
- Fraud – Inaccurate information within databases, logs, files or paper records
- Abnormal system behavior (e.g., unscheduled system reboot, unexpected messages, abnormal errors in system log files or on terminals)
- Security event notifications (e.g., file integrity alerts, intrusion detection alarms, and physical security alarms)

All employees, regardless of job responsibilities, should be aware of the potential incident identifiers and who to notify in these situations. In all cases, every employee should report incidents per the instructions under Incident Reporting, unless they are assigned other activities within the incident response plan.

13. HARD COPY STORAGE REQUIREMENTS. Hard copy materials containing Sensitive Information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:

    - At no time are printed reports containing Sensitive Information to be removed from the secure office environment.
    - All hardcopy material containing Sensitive Information should be clearly labeled as such.
    - All hardcopy media which contains Sensitive Information must be stored in a secure and locked container (e.g. locker, cabinet, desk, storage bin). Sensitive Information is never to be stored in unlocked or unsecured containers or open workspaces.
    - All Sensitive Information, when no longer needed for legal, regulatory or business requirements must be disposed of in hardcopy shred bins. All hardcopy shred bins must remain locked at all times (until shredding.)

14. WORKSTATION PROTECTION. When an employee who has access to Sensitive Information at their work station leaves the work station, for any duration of time, the employee is responsible for removing all Sensitive Information from their desk and placing it in a locked secure area. Should a user forget to do one of the above aforementioned; the workstation should be set up to automatically hibernate, turn off hard drives and require a password upon return.

    Passwords to computers should be changed every 90 days. This password is comprised of at least 8 alpha-numeric characters, both upper and lower case letters, and numbers. If an employee believes their password has been compromised, they must immediately report to the Privacy Officer to have a new password generated.

    Absolutely no Sensitive Information can be left at a work station or in an open area after closing. Each employee will apply this policy as if the office was completely closed at the end of the shift. At the close of business each day, all employees are required to lock all Sensitive Information in assigned cabinets. Group printers must be checked before an employee leaves

for the day to ensure no Sensitive Information remains at the printing station. All mailboxes must also be checked each evening before leaving. All storage, file cabinets and doors are to be locked at all times, unless in direct use. Workstations are restricted from any unauthorized use by visitors. Workstations that could be accessible by office visitors must have privacy filters on all monitors and be locked at all times when not in use.

15. LAPTOP USE AND SECURITY. Employees are not permitted to have Sensitive Information on their Laptops unless it is for a limited purpose and is coordinated by the Privacy Officer. After the limited purpose has been completed, the Sensitive Information should be deleted from the Laptop to the extent possible. Laptops that contain Sensitive Information are to be password protected, locked when out of the office or at a location where a third party may gain access including their home, or any offsite location. In the event a laptop containing Sensitive Information is lost or stolen, the employee must immediately notify the Privacy Officer who will perform a risk assessment.

    Passwords to computers should be changed every 90 days. This password is comprised of at least 8 alpha-numeric characters, both upper and lower case letters, and numbers. If an employee believes their password has been compromised, they must immediately report to the Privacy Officer to have a new password generated.

16. ELECTRONIC DATA RETENTION AND STORAGE REQUIREMENTS – WRITABLE MEDIA. Sensitive Information can be stored in an electronic manner. Electronic media containing Sensitive Information (e.g., CD, DVD, floppy disk, hard disk, tape, etc.) are subject to this Privacy Policy Security Rule. At no time is electronic Sensitive Information to be removed from the secure office environment, except for computer system backups or as allowed under this Policy. Sensitive Information will be physically retained, stored or archived only within secure office environment, and only for the minimum time deemed necessary for its use. Any download of Sensitive Information to a device taken outside the secure office environment must be completed, with the knowledge of the Privacy Officer, for the purpose of HCS administration. Any violation of this Policy can be subject to discipline, including termination of employment.

17. SENSITIVE INFORMATION DESTRUCTION REQUIREMENTS. All Sensitive Information no longer needed for HCS facilitation must be destroyed. Copies of the Sensitive Information may, if necessary, be stored for 6 years in a secure environment.

    Before any electronic device that received, transmitted or stored Sensitive Information can be sent to a vendor for trade-in, servicing or disposal, all Sensitive Information will be destroyed or removed and rendered unrecoverable. Removable computer storage media such as floppy, optical disks or magnetic tapes may not be donated to charity or otherwise recycled.

    Physical copies of Sensitive Information no longer needed will be destroyed typically through shredding. Outsourced destruction of Sensitive Information may be by performed by a bonded Disposal Vendor that provides a "Certificate of Destruction". Other documented approaches can be used if they show the physical destruction of the data. The Privacy Officer must give written permission to approve methods of destruction of Sensitive Information not described within this Privacy Policy.

18. ACCESS MANAGEMENT AND CONTROL POLICY. Access to Sensitive Information is limited to employees who have completed Privacy Policy training. It is one purpose of this policy to identify access points and address appropriate usage of Sensitive Information. This Policy addresses physical access for employees, vendors and visitors. This Policy also covers appropriate usage/access to external media. By restricting access. the likelihood of a Breach by malicious or non-malicious acts is reduced. An employee's access to Sensitive Information shall be determined by the Privacy Officer and authorized according to business needs. User access to computer resources shall be provided only when necessary to perform tasks related to business.

19. FIREWALL. Sedera has established appropriate administrative, technical, and physical safeguards ("Firewalls") to prevent Sensitive Information from intentionally or unintentionally being used or disclosed in violation of this Privacy Policy's requirements. The Firewalls ensure only authorized employees have access to Sensitive Information. By following the secure process outlined in this Policy, Sensitive Information received will not be shared with any employee who is not trained on this Privacy Policy or who has no HCS purpose for access.

    Only employees who are trained on this Policy and have a business purpose related to a HCS function can have access to Sensitive Information, and only the data that is necessary to complete that function is permitted to be accessed.

20. VISITORS. Physical access to any area where Sensitive Information, electronic or otherwise, is maintained will be under strict supervision. Visitors must be accompanied by an employee while in the area where Sensitive Information is maintained. Employees who accompany Visitors must be sure that the areas that they visit are void of Sensitive Information. Prior announcements to areas that typically deal with Sensitive Information may be needed to ensure that Sensitive Information is not exposed to Visitors.

21. AUTOMATIC AMENDMENTS. Any term or item in this Privacy Policy will automatically be amended to comply with changes in any applicable federal laws and regulations. This Privacy Policy will be updated once yearly.

22. State Specific Rules: Each of the 50 states maintains various standards for information privacy. Sedera is committed upholding all applicable laws related to safeguarding Sensitive Information in the states in which it operates. Your rights may vary from state to state; to the degree your privacy rights are more protective, your individual state statute will supersede this policy.