



STATE OF IOWA
MASTER AGREEMENT
Contract Declaration and Execution

MA 005

20242

EFFECTIVE BEGIN DATE: 02-10-2020
EXPIRATION DATE: 02-09-2022
PAGE: 1 of 3

VENDOR:

GREEN RESOURCE MANAGEMENT VENDOR CONTACT:
INC

THE SHREDDER

Nick Poulter

PHONE: 5152803013

1000 THOMAS BECK RD
DES MOINES, IA 50315-1060

EMAIL: nick@the-shredder.com

ISSUER:

Kelli Sizenbach

EXT: PHONE: 515-725-2275

EMAIL: Kelli.Sizenbach@iowa.gov

FOB:

Contract For: Secure Document Shredding Services

The parties agree to comply with the terms and conditions on the following attachments which are by this reference made a part of the Agreement.

Attachments are on file with the Department of Administrative Services - Central Procurement.

Attachment 1: Competitive Solicitation RFP1420005036.

Attachment 2: Contractor's Response to Competitive Solicitation RFP14.

Attachment 3: Signed BAA

Sales Contact Information
Andrew Sloan
515-280-3013 x2002
Andrew@the-shredder.com

RENEWAL OPTIONS

FROM 02-10-2022 **TO** 02-09-2023

FROM 02-10-2023 **TO** 02-09-2024

FROM 02-10-2024 **TO** 02-09-2025

FROM 02-10-2025 **TO** 02-09-2026

AUTHORIZED DEPARTMENT

ALL

SUB Other Governmental Entities



STATE OF IOWA
MASTER AGREEMENT
Contract Declaration and Execution

MA 005

20242

EFFECTIVE BEGIN DATE: 02-10-2020

EXPIRATION DATE: 02-09-2022

PAGE: 2 of 3

LINE NO.	QUANTITY / SERVICE DATES	UNIT	COMMODITY / DESCRIPTION	UNIT COST / PRICE OF SERVICE
----------	--------------------------	------	-------------------------	------------------------------

1	0.00000	EA	96227	
				\$ 0.000000
				\$ 0.000000

REF DOC:

REF VNDR LN:

REF COMM LN:

REF TYPE: FINAL

Document Shredding Services

Document Shredding Services

Pick-ups must be signed for and end users must receive destruction confirmation. All documents must remain confidential at all times.

\$10 per bin (32, 65 or 95 gallon)

2	0.00000	EA	96227	
				\$ 0.000000
				\$ 0.000000

REF DOC:

REF VNDR LN:

REF COMM LN:

REF TYPE: FINAL

Document Shredding Services

Emergency Services

Emergency document shred services \$100 sur charge.

3	0.00000	EA	96227	
				\$ 0.000000
				\$ 0.000000

REF DOC:

REF VNDR LN:

REF COMM LN:

REF TYPE: FINAL

Document Shredding Services

Purge Services

Purge shred services \$4 per box.



STATE OF IOWA
MASTER AGREEMENT
Contract Declaration and Execution

MA 005

20242

EFFECTIVE BEGIN DATE: 02-10-2020
EXPIRATION DATE: 02-09-2022
PAGE: 3 of 3

TERMS AND CONDITIONS

Services Effective 1 May 16

The parties agree to comply with the terms and conditions on the following web site which are by this reference made a part of the Agreement. General Terms and Conditions for service contracts are posted at: <https://das.iowa.gov/sites/default/files/procurement/pdf/050116%20terms%20services.pdf>

THIS MASTER AGREEMENT IS EFFECTIVE AS OF THE LATEST DATE SHOWN IN "EFFECTIVE BEGIN DATE" IN THE UPPER RIGHT HAND CORNER OR THE DATE BELOW SIGNED BY THE STATE OF IOWA.

CONTRACTOR		STATE OF IOWA	
CONTRACTOR'S NAME (If other than an individual, state whether a corp, partnership, etc.) <i>THE SHREDDER</i>		AGENCY NAME DAS Central Procurement Bureau	
BY (Authorized Signature)	Date Signed <i>2/11/2020</i>	BY (Authorized Signature)	Date Signed <i>2/12/2020</i>
Printed Name and Title of Person Signing <i>U.P.</i>		Printed Name and Title of Person Signing <i>Helli Sizenbach</i> -Purchasing Agent	
Address <i>1000 THOMAS BECK RD DES MOINES, IA, 50315</i>		Address Hoover Bldg 3rd Floor 1305 E Walnut St Des Moines Iowa 50319-0105	

Attachment #8
Iowa Department of Revenue
Confidential Information Requirements for Contractors
ONLY NECESSARY FOR REGIONS 1 & 2

8.1 Access to Confidential Data

The contractor's employees, agents, and subcontractors may have access to confidential data maintained by the Iowa Department of Revenue (hereafter referred to as 'IDR' or 'the Department') to the extent necessary to carry out its responsibilities under the Contract. The contractor shall presume that all information received pursuant to the Contract is confidential unless otherwise designated by the Department.

8.2 Performance

In performance of the Contract, the contractor agrees to comply with and assume responsibility for compliance by its employees, agents, or subcontractors with the following requirements:

- 8.2.1 All work will be done under the supervision of the contractor or the contractor's employees. The contractor must designate one individual who shall remain the responsible authority in charge of all data collected, used, or disseminated by the contractor in connection with the performance of its duties under the Contract.

The contractor shall provide adequate supervision and training to its employees, agents, or subcontractors to ensure compliance with the terms of the Contract. Annual training shall include, but is not limited to, the IRS video "Protecting Tax Information".

The contractor shall provide acceptance by its employees, agents, or subcontractors, by signature, of the terms of federal and state confidentiality disclosure (see Exhibit 1 Acknowledgment of Statements of Confidentiality).

The contractor shall provide to the Department a written description of its policies and procedures to safeguard confidential information. Policies of confidentiality shall address, as appropriate, information conveyed in verbal, written, and electronic formats.

The contractor will maintain a list of employees, agents, or subcontractors with authorized access to the Department's data. Such list will be provided to IDR and, when federal tax information (FTI) is involved, to the Internal Revenue Service (IRS) reviewing office upon request.

The contractor and the contractor's employees, agents, and subcontractors with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.

No work furnished under this Contract will be subcontracted without prior written approval from the Department. If written approval is received, all subcontractors and subcontractor's employees shall be held to the same standards as the contractor and the contractor's employees, including, but not limited to, annual training and acceptance of confidentiality disclosure.

No data can be accessed by contractor, or contractor's employees, agents, and subcontractors located offshore or via any information systems located off-shore.

The contractor will complete a security risk assessment questionnaire annually, as part of a certification process with the Department.

- 8.2.2 Any tax information made available in any format shall be used only for the purpose of carrying out the provisions of this Contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of its duties under this Contract. Inspection by or disclosure to anyone other than an authorized officer, employee, agent or subcontractor of the contractor is prohibited.
- 8.2.3 All tax information will be accounted for upon receipt and properly safeguarded in accordance with security requirements set forth in this Contract before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.
- 8.2.4 Upon completion of duties under this Contract or the specific direction of IDR, the contractor will certify that the data processed and any output generated during the performance of duties under this Contract will be completely purged from all data storage components, including, but not limited to data center facility, laptops, computers and other storage devices. If immediate purging of all data storage components is not possible, the contractor will certify that any tax information remaining in any storage component will be safeguarded to prevent unauthorized disclosures until it has been purged. Once all data processed and output generated has been completely purged, the contractor shall submit a signed certification to the Department to that effect.
- 8.2.5 Any spoilage or intermediate hardcopy output that may result during the processing of tax information will be given to the Department. When this is not possible, the contractor will be responsible for the destruction of the spoilage or intermediate hard copy printouts, and will provide the Department with a statement containing the date of destruction, description of material destroyed, and the method used. Destruction method must meet specifications as defined in IRS Publication 1075 Section 8.3.
- 8.2.6 The contractor will ensure that all computer systems processing, storing, or transmitting tax information meets the computer system security requirements defined in IRS Publication 1075 Section 9.1. The security features of the computer systems must meet all functional and assurance requirements for the managerial, operational, and technical security controls. All security features must be available and activated to protect against unauthorized use of and access to tax information.
- 8.2.7 The use of personally owned computers for accessing IDR information is strictly prohibited.
- 8.2.8 Any data supplied by IDR to the contractor or contractor's employees, agents, or subcontractors or created by the contractor or contractor's employees, agents, or subcontractors in the course of the performance of its duties under this Contract shall be

considered the property of IDR. No confidential information collected, maintained, or used in the course of performance of the Contract shall be disseminated by the contractor or contractor's employees, agents, or subcontractors except as authorized by law and only with the prior written consent of the Department, either during the period of the Contract or thereafter. The contractor may be liable for an unauthorized disclosure if it fails to comply with federal and state confidential safeguard requirements.

- 8.2.9 In the event that a subpoena or other legal process is served upon the contractor for records containing confidential information, the contractor shall promptly notify IDR and cooperate with the Department in any lawful effort to protect the confidential information.
- 8.2.10 The contractor shall immediately report to IDR any unauthorized disclosure or security breach of confidential information. These include, but are not limited to: (i) Unauthorized access or disclosure of confidential information; (ii) Illegal technology transfer; (iii) Sabotage, destruction, theft, or loss of confidential information or the information systems, and (iv) Compromise or denial of confidential information or information systems.
- 8.2.11 IDR and the IRS, with 24 hour notice, shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under this Contract for compliance with requirements defined in IRS Publication 1075. The IRS's right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. An inspection questionnaire may be used in lieu of an on-site visit at the discretion of the IRS. On the basis of such inspection, specific actions may be required of the contractor in cases where the contractor is found to be noncompliant with Contract safeguards.
- 8.2.12 If the Department is required to notify taxpayers of a security or confidentiality breach caused by the contractor, the Department is entitled to reimbursement of such costs related to this notification from the contractor (see Iowa Code § 715C.2).
- 8.2.13 If the contractor fails to provide the safeguards described above, IDR will have the right to void the Contract immediately.
- 8.2.14 The contractor's confidentiality obligations under this section shall survive the termination of this Contract.
- 8.2.15 Any disclosure of federal tax information shall be subject to penalties prescribed by IRC §§ 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1. Any disclosure of state tax information as governed by the Iowa Code Ann., §§ 422.20, 422.72, and 452A.63, shall be subject to penalties prescribed therein.

8.3 Criminal/Civil Sanctions

- 8.3.1 Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing that returns or return information disclosed to such

officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Each officer and employee shall be further notified that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC §§7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

- 8.3.2 Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Agreement. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the Agreement. Inspection by any unauthorized person constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Each such officer and employee shall be notified that any such unauthorized inspection of returns or return information may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of \$1,000 for each act of unauthorized inspection with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection plus in the case of a willful inspection which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRC §§ 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.
- 8.3.3 Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.
- 8.3.4 Granting a contractor access to FTI must be preceded by certifying that each individual understands IDR's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in IDR's files for review. As part of the certification and at least annually afterwards, the contractor shall be advised of the provisions of IRC §§7213, 7213A, and 7431. The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches (See Publication 1075 Section 10). For both the initial certification and the annual certification, the contractor's employees, agents, and

subcontractors shall sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

Acknowledgment of Statement of Confidentiality


Release of Confidential Internal Revenue Service (IRS) Information

Pursuant to the agreement between the State of Iowa and the IRS, I realize that information provided the Iowa Department of Revenue by the Department of Treasury is confidential in nature. I am also aware that the following is punishable:

- 1) The willful inspection (browsing) of information without authorization, or
- 2) The willful release of such information to persons other than that intended by Iowa Department of Revenue policy and procedures.

A person committing an offense of willful inspection without authorization of federal information against the provisions of Section 7213 A of the Internal Revenue Code shall be guilty of a federal misdemeanor and, upon conviction thereof, shall be fined not more than \$1,000 or imprisoned not more than one year, or both, together with the cost of prosecution.

A person committing an offense of unauthorized disclosure of federal information against the provisions of Sections 6103 and 7213(a) of the Internal Revenue Code shall be guilty of a felony and, upon conviction thereof, shall be fined not more than \$5,000 or imprisoned not more than five years, or both, together with the cost of prosecution. In addition, a person may be subject to civil action by the taxpayer for unlawful inspection or disclosure pursuant to section 7431 of the Internal Revenue Code.


Employee's Initials

Release of Confidential Iowa Department of Revenue Information

Pursuant to the Code of Iowa, I understand the willful release of confidential information in a manner inconsistent with Iowa law is punishable as set forth below. I also understand that the willful inspection (browsing) of tax records is a violation of Iowa law. A person committing an offense against the above provisions shall be guilty of a serious misdemeanor and, upon conviction thereof, shall be fined up to \$1,000 and/or imprisoned up to one year. In addition, that person will be discharged from employment and may face the potential of personal liability in a lawsuit brought by the affected taxpayer.


Employee's Initials

My understanding of these obligations is acknowledged by my initials above and my signature here.

ANDREW SLOAN
Print Name


Signature

2-11-20
Date

THE SHREDDER
IDR Division / Company Name

**Iowa Department of Human Services
Business Associate Agreement
*NECESSARY FOR ALL REGIONS***

THIS Business Associate Agreement ("BAA") supplements and is made a part of the Contract (hereinafter, the "Underlying Agreement") between the Iowa Department of Human Services (the "Agency") and the Contractor (the "Business Associate").

1. Purpose

The Business Associate performs certain services on behalf of or for the Agency pursuant to the Underlying Agreement that may include the exchange of information that is protected by the Health Insurance Portability and Accountability Act of 1996, as amended, and the HIPAA Rules (collectively "HIPAA"). The parties to the Underlying Agreement are entering into this BAA to establish the responsibilities of both parties regarding Protected Health Information and to bring the Underlying Agreement into compliance with HIPAA.

2. Definitions

The following terms used in this BAA shall have the same meaning as those terms in the HIPAA Rules: Breach, Designated Record Set, Disclose, Disclosure, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

- a. **"Business Associate"** shall generally have the same meaning as the term "Business Associate" at 45 C.F.R. § 160.103, and in reference to the party to this BAA, shall mean the Contractor.
- b. **"Covered Entity"** shall generally have the same meaning as the term "covered entity" at 45 C.F.R. § 160.103, and in reference to the party to this BAA shall mean the portions of the Agency, which is a "hybrid" entity under HIPAA, that fall under the purview of HIPAA.
- c. **"HIPAA Rules"** shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164.

3. Obligations and Activities of Business Associate

The Business Associate agrees to:

- a. Not Use or Disclose Protected Health Information other than as permitted or required by this BAA or as Required By Law;
- b. Use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to Protected Health Information, to prevent Use or Disclosure of Protected Health Information other than as provided for by this BAA;
- c. Report to the Covered Entity any Use or Disclosure of Protected Health Information not provided for by this BAA of which it becomes aware, including Breaches of Unsecured Protected Health Information as required at 45 C.F.R. § 164.410, and any security incident of which it becomes aware in accordance with subsection 7, below;
- d. In accordance with 45 C.F.R. § 164.502(e)(1)(ii) and 45 C.F.R. § 164.308(b)(2), if applicable, ensure that any Subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information;

- e. Make available Protected Health Information in a Designated Record Set to the Covered Entity as necessary to satisfy the Covered Entity's obligations under 45 C.F.R. §164.524;
- f. Make any amendment(s) to Protected Health Information in a Designated Record Set as directed or agreed to by the Covered Entity pursuant to 45 C.F.R. §164.526, or take other measures as necessary to satisfy the Covered Entity's obligations under 45 C.F.R. § 164.526;
- g. Maintain and promptly make available, as directed by the Covered Entity, the information required to provide an accounting of Disclosures to the Covered Entity as necessary to satisfy the Cover Entity's obligations under 45 C.F.R. § 164.528;
- h. Immediately (i.e., within 72 hours) forward any request that the Business Associate receives directly from an Individual who (1) seeks access to Protected Health Information held by the Business Associate pursuant to this BAA, (2) requests amendment of Protected Health Information held by the Business Associate pursuant to this BAA, or (3) requests an accounting of Disclosures, so that the Covered Entity can coordinate the response;
- i. To the extent the Business Associate is to carry out one or more of the Covered Entity's obligation(s) under Subpart E of 45 C.F.R. Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s); and
- j. Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

4. Permitted Uses and Disclosures by the Business Associate.

- a. The Business Associate may Use or Disclose Protected Health Information received in relation to the Underlying Agreement as necessary to perform the services set forth in the Underlying Agreement.
- b. The Business Associate is not authorized to de-identify Protected Health Information in accordance with 45 C.F.R. § 164.514(a)-(c) unless expressly authorized to do so in writing by the Covered Entity's Security and Privacy Officer.
- c. The Business Associate agrees to make Uses and Disclosures and Requests for Protected Health Information consistent with the Covered Entity's Minimum Necessary policies and procedures.
- d. The Business Associate may not Use or Disclose Protected Health Information in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by the Covered Entity.
- e. The Business Associate may Use or Disclose the Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided the Disclosures are Required By Law, or the Business Associate obtains reasonable assurances from the person to who 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 Protected Health Information has been Breached.

5. Obligations of the Covered Entity

- a. The Covered Entity will notify the Business Associate of any limitation(s) in the Notice of Privacy Practices of Covered Entity under 45 C.F.R. § 164.520, to the extent that such limitation may affect the Business Associate's Use or Disclosure of Protected Health Information.

- b. The Covered Entity will notify the Business Associate of any changes in, or revocation of, the permission by an Individual to Use or Disclose his or her Protected Health Information, to the extent that such changes may affect the Business Associate's Use or Disclosure of Protected Health Information.
- c. The Covered Entity shall notify the Business Associate of any restriction on the Use or Disclosure of Protected Health Information that the Covered Entity has agreed to or is required to abide by under 45 C.F.R. § 164.522, to the extent that such restriction may affect the Business Associate's Use or Disclosure of Protected Health Information.

6. Permissible Requests by the Covered Entity

The Covered Entity shall not request the Business Associate to Use or Disclose Protected Health Information in any manner that would not be permissible under Subpart E of 45 C.F.R. Part 164 if done by the Covered Entity.

7. Breach Notification Obligations of the Business Associate

In the event that the Business Associate discovers a Breach of Unsecured Protected Health Information, the Business Associate agrees to take the following measures immediately (i.e., within 72 hours) after the Business Associate first discovers the incident:

- a. To notify the Covered Entity of any Breach. Such notice by the Business Associate shall be provided without unreasonable delay, except where a law enforcement official determines that a notification would impede a criminal investigation or cause damage to national security. For purposes of this BAA, the Business Associate is deemed to have discovered the Breach as of the first day on which such Breach is known to the Business Associate or by exercising reasonable diligence, would have been known to the Business Associate, including any person, other than the Individual committing the Breach, that is a workforce member or agent of the Business Associate;
- b. To include to the extent possible the identification of the Individuals whose Unsecured Protected Health Information has been, or is reasonably believed to have been, the subject of a Breach;
- c. To complete and submit the DHS Incident Report form located on the Agency's website at <https://dhs.iowa.gov/hipaa/baa>; and
- d. To draft a letter for the Covered Entity to utilize to notify the Individuals that their Unsecured Protected Health Information has been, or is reasonably believed to have been, the subject of a Breach. The draft letter must include, to the extent possible:
 - i. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;
 - ii. A description of the types of Unsecured Protected Health Information that were involved in the Breach (such as full name, Social Security Number, date of birth, home address, account number, disability code, or other types of information that were involved);
 - iii. Any steps the Individuals should take to protect themselves from potential harm resulting from the Breach;
 - iv. A brief description of what the Covered Entity and the Business Associate are doing to investigate the Breach, to mitigate harm, and to protect against any further Breaches; and
 - v. Contact procedures for Individuals to ask questions or learn additional information, which shall include Covered Entity contact information, including a toll-free telephone number, an e-mail address, web site, or postal address.

8. BAA Administration

a. Term and Termination

This BAA is effective on the date of its incorporation into the Underlying Agreement. The Covered Entity may terminate this BAA for cause if the Covered Entity determines that the Business Associate or any of its Subcontractors or agents has breached a material term of this BAA. The Covered Entity will provide written notice to the Business Associate requesting that the Business Associate remedy the breach within the time frame provided in the notice. The remedy time frame provided the Business Associate will be consistent with the severity of the breach. The Covered Entity reserves the right to terminate the BAA without notice in the event that the Covered Entity determines, in its sole discretion, that notice is either infeasible or inappropriate under the circumstances. Expiration or termination of either the Underlying Agreement or this BAA shall constitute expiration or termination of the corresponding agreement.

b. Obligation to Return PHI, Destroy PHI, or Extend Protections to Retained PHI

Upon expiration or termination of this BAA for any reason, the Business Associate shall return to the Covered Entity or destroy all Protected Health Information received from Covered Entity, or created, maintained, or received by the Business Associate on behalf of the Covered Entity, that the Business Associate still maintains in any form. Return or destruction of Protected Health Information shall take place in accordance with the requirements for such return or destruction as set forth in the Underlying Agreement or as otherwise directed by the Covered Entity. The Business Associate shall retain no copies of the Protected Health Information unless such return or destruction is not feasible. If return or destruction of the Protected Health Information is not feasible, upon expiration or termination of this BAA, the Business Associate shall:

- i. Retain only that Protected Health Information that is necessary for the Business Associate to continue its proper management and administration or to carry out its legal responsibilities to the extent Required By Law;
- ii. Return to the Covered Entity or destroy the remaining Protected Health Information that the Business Associate still maintains in any form;
- iii. Continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to Protected Health Information to prevent Use or Disclosure of the Protected Health Information, other than as provided for in this Section, for as long as the Business Associate retains the Protected Health Information;
- iv. Not Use or Disclose the Protected Health Information retained by the Business Associate other than for the purposes for which such Protected Health Information was retained and subject to the same conditions set out in subsection 4(e) above under "Permitted Uses and Disclosures by the Business Associate" which applied prior to termination; and
- v. Return to the Covered Entity or destroy the Protected Health Information retained by the Business Associate when it is no longer needed by the Business Associate for its proper management and administration or to carry out its legal responsibilities.

c. **Compliance with Confidentiality Laws**

The Business Associate acknowledges that it must comply with all applicable laws that may protect the Protected Health Information or other patient information received and will comply with all such laws, which include but are not limited to the following:

- i. Medicaid applicants and recipients: 42 U.S.C. § 1396a(a)(7); 42 C.F.R. §§431.300 - .307; Iowa Code § 217.30;
- ii. Mental health treatment: Iowa Code chapters 228, 229;
- iii. HIV/AIDS diagnosis and treatment: Iowa Code § 141A.9;
- iv. Substance abuse treatment: 42 U.S.C. § 290dd-2; 42 C.F.R. part 2; Iowa Code §§ 125.37, 125.93.v.Consumer personal information: Iowa Code ch. 715C.

d. **Financial Obligations for Breach Notification**

- i. To the extent that the Business Associate is a governmental agency subject to the provisions of Iowa Code § 679A.19, any dispute between the Contractor and the Agency, including but not limited to the incursion of any costs, liabilities, damages, or penalties related to the Business Associate's breach of this BAA, shall be submitted to a board of arbitration in accordance with Iowa Code §679A.19.
- ii. To the extent that the Business Associate is not subject to the provisions of Iowa Code § 679A.19, the Business Associate shall defend, indemnify, and hold harmless the Covered Entity from costs, liabilities, damages, or penalties incurred as a result the Business Associate or any Subcontractor's breach of this BAA, the Underlying Agreement, or conduct of the Business Associate or the Business Associate's Subcontractor that is not in compliance with 45 C.F.R. Part 164,subpart E. Such liability shall not attach to disclosures made at the express written direction of the Covered Entity.
- iii. The Business Associate's obligations under this subsection 8(d) are not limited to third-party claims but shall also apply to claims by the Covered Entity against the Business Associate.

e. **Amendment**

The Covered Entity may amend the BAA from time to time by posting an updated version of the BAA on the Agency's website at: <https://dhs.iowa.gov/hipaa/baa>, and providing the Business Associate electronic notice of the amended BAA. The Business Associate shall be deemed to have accepted the amendment unless the Business Associate notifies the Covered Entity of its non-acceptance in accordance with the Notice provisions of the Contract within 30 days of the Covered Entity's notice referenced herein. Any agreed alteration of the then current Covered Entity BAA shall have no force or effect until the agreed alteration is reduced to a Contract amendment and signed by the Contractor, Agency Director, and the Agency Security and Privacy Officer.

f. **Survival**

All obligations of the Agency and the Business Associate incurred or existing under this BAA as of the date of expiration or termination will survive the expiration or termination of this BAA.

g. **No Third Party Beneficiaries**

There are no third party beneficiaries to this BAA between the parties. The Underlying Agreement and this BAA are intended to only benefit the parties to the BAA.

h. Miscellaneous

i. Regulatory References

A reference in this BAA to a section in the HIPAA Rules means the section as it may be amended from time to time.

ii. Interpretation

Any ambiguity in this BAA shall be interpreted to permit compliance with the HIPAA Rules.

iii. Applicable Law

Except to the extent preempted by federal law, this BAA shall be governed by and construed in accordance with the same internal laws as that of the Underlying Agreement.

Attachment #9

Confidentiality Acknowledgements

The Contractor shall acknowledge by signature, acceptance by its employees, agents, or subcontractors of the terms of federal and state confidentiality disclosure provisions in Internal Revenue Service Confidential Information Safeguarding Provisions, Confidential Information Safeguarding Provisions and Acknowledgement of Statement of Confidentiality.

Internal Revenue Service Confidential Information Safeguarding Provisions

I. PERFORMANCE

In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

- (1) All work will be performed under the supervision of the contractor or the contractor's responsible employees.
- (2) The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.
- (3) Any Federal tax returns or return information (hereafter referred to as returns or return information) made available shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the contractor is prohibited.
- (4) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.
- (5) No work involving returns and return information furnished under this contract will be subcontracted without prior written approval of the IRS.
- (6) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.
- (7) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.
- (8) (Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

- (1) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as five years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.
- (2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information

contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000.00 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of \$1,000.00 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRCs 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs 7431, 7213, and 7213A (see Exhibit 4, *Sanctions for Unauthorized Disclosure*, and Exhibit 5, *Civil Damages for Unauthorized Disclosure*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with contract safeguards.

Definition of Confidential Information. The term “Confidential Information” shall include, but not be limited to, the following:

- All individual case information received pursuant to this Contract unless otherwise designated by the Bureau,
- An individual’s social security number,
- An individual’s residential and mailing addresses,
- An individual’s employment information, and
- An individual’s financial information.

Prohibitions against the Use and Disclosure of Confidential Information. The Contractor shall not use, handle, transmit, store, or destroy the Confidential Information of applicants or recipients of child support enforcement services in a manner or for any purpose, except as allowed by the provisions of the Contract. The Contractor shall safeguard the confidentiality of Confidential Information concerning applicants or recipients of child support enforcement services according to 5 U.S.C. § 552a; 26 U.S.C. § 6103; 42 U.S.C. §§ 654 and 654a; Iowa Code § 252B.9; Iowa Code Chapter 715C; 45 CFR Parts 303.21 and 307.13; and other applicable federal and state laws.

Internal Revenue Service Data. The Contractor shall adhere to the safeguarding provisions of *Internal Revenue Service Publication 1075*. Exhibit F contains a summary of the Contractor’s Confidential Information safeguarding requirements and penalties pertaining to Internal Revenue Service information.

Reporting. The Contractor shall report to the Bureau’s Security and Privacy Officer and the Child Support Recovery Unit any use or disclosure of the Confidential Information not provided for by this Contract of which the Contractor becomes aware, as well as report any suspected or unauthorized access to or disclosure of Confidential Information. The Contractor agrees to report suspected or unauthorized access to or disclosure of Confidential Information immediately, as the Bureau is required to report the suspected or unauthorized access or disclosure within the following timeframes:

- Federal Tax Information24 hours
- Social Security Information1 hour
- Federal Parent Locator Service1 hour
- All other Confidential Information3 Business Days

Sanctions. State and federal statutes carry criminal penalty or civil liability for confidentiality violation. For example, see Iowa Code § 252B.10; 5 U.S.C. § 552a; 42 U.S.C. §§ 653(l)(2) and 654a(d)(5); and 26 U.S.C. §§ 7213A and 7431. The Contractor may not use the Confidential Information for commercial or political purposes or re-disclose the Confidential Information without the express, written consent of the Bureau. The Contractor may be held civilly or criminally liable for misuse of the Confidential Information.

Survival. The provisions of the Contract that protect Confidential Information shall survive termination of the Contract.

Acknowledgement of Statement of Confidentiality

I understand all information received under this contract is confidential unless otherwise designated by the Agency. I further understand I am bound by state and federal confidentiality law that prohibits disclosure of state and federal data and program information. For example, see Iowa Code section 252B.9 and 252B.9A. Some of these statutes carry criminal penalty or civil liability for statute violation. For example, see Iowa Code section 252B.10, 42 U.S.C. §653(l)(2) and 654a(d)(5), and 5 U.S.C. § 552a.

I realize that information provided to the Department of Human Services by the Internal Revenue Service is confidential in nature. I am also aware the following is punishable:


- 1) The willful inspection (browsing) of information without authorization, or
- 2) The willful release of such information to persons other than that intended by the Iowa Department of Human Services policy and procedures.

I understand unauthorized inspection of federal tax information to anyone against the provisions of Section 7213A and 7431 of the Internal Revenue Code is a criminal misdemeanor punishable, upon conviction, by a fine of as much as \$1,000.00 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. I further understand that any such unauthorized inspection I am found to be responsible for may also result in a money judgment against me in an amount equal to the sum of the greater of \$1,000 for each unauthorized inspection or the amount of the actual damages to the taxpayer.

I understand unauthorized willful disclosure of federal tax information to anyone against the provisions of Section 7213 and 7431 of the Internal Revenue Code is a felony punishable if convicted by a fine up to \$5,000 or imprisonment up to five (5) years, or both, plus the cost of prosecution. I further understand that any such unauthorized future disclosure of federal tax information may also result in a money judgment against me in an amount not less than \$1,000 for each unauthorized disclosure.

I also understand that under 5 U.S.C. § 552a, The Privacy Act of 1974, willful disclosure of SSA information can result in a misdemeanor and a fine not to exceed \$5,000. Willful maintenance of a system of records can result in a misdemeanor and fine not to exceed \$5,000. Willfully and knowingly requesting or obtaining records under false pretenses can result in a misdemeanor and fine not to exceed \$5,000.

I have read and understand this Acknowledgement of Statement of Confidentiality Information and have had an opportunity to ask my supervisor questions about this information.

Printed Name ANDREW SLOAN	Company Name THE SHREDDER
Signature 	Date 2-11-20