



## HIPAA POLICIES AND PROCEDURES

### I. POLICY

A. It is the policy of ACTION REVENUE RECOVERY, LLC that information, as defined hereinafter, in all its forms--written, spoken, recorded electronically or printed--will be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information.

B. All policies and procedures must be documented and made available to individuals responsible for their implementation and compliance. All activities identified by the policies and procedures must also be documented. All the documentation, which may be in electronic form, must be retained for at least 6 (six) years after initial creation, or, pertaining to policies and procedures, after changes are made. All documentation must be periodically reviewed for appropriateness and currency, a period of time to be determined by each entity within ACTION REVENUE RECOVERY, LLC.

C. At each entity and/or department level, additional policies, standards and procedures will be developed detailing the implementation of this policy and set of standards, and addressing any additional information systems functionality in such entity and/or department. All departmental policies must be consistent with this policy. All systems implemented after the effective date of these policies are expected to comply with the provisions of this policy where possible. Existing systems are expected to be brought into compliance where possible and as soon as practical.

### II. SCOPE

A. The scope of information security includes the protection of the confidentiality, integrity and availability of information.

B. The framework for managing information security in this policy applies to all ACTION REVENUE RECOVERY, LLC entities and workers, and other Involved Persons and all Involved Systems throughout ACTION REVENUE RECOVERY, LLC as defined below in INFORMATION SECURITY DEFINITIONS.

C. This policy and all standards apply to all protected health information and other classes of protected information in any form as defined below in INFORMATION CLASSIFICATION.

### III. RISK MANAGEMENT

A. A thorough analysis of all ACTION REVENUE RECOVERY, LLC information networks and systems will be conducted on a periodic basis to document the threats and vulnerabilities to stored and transmitted information. The analysis will examine the types of threats, internal or external, natural or manmade, electronic and non-electronic-- that affect the ability to manage the information resource. The analysis will also document the existing vulnerabilities within each entity which potentially expose the information resource to the threats. Finally, the analysis will also include an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection. From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined. The frequency of the risk analysis will be determined at the entity level.

B. Based on the periodic assessment, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities.

### IV. INFORMATION SECURITY DEFINITIONS

**Affiliated Covered Entities:** Legally separate, but affiliated, covered entities which choose to designate themselves as a single covered entity for purposes of HIPAA.

**Availability:** Data or information is accessible and usable upon demand by an authorized person.

**Confidentiality:** Data or information is not made available or disclosed to unauthorized persons or processes.

**HIPAA:** The Health Insurance Portability and Accountability Act, a federal law passed in 1996 that affects the healthcare and insurance industries. A key goal of the HIPAA regulations is to protect the privacy and confidentiality of protected health information by setting and enforcing standards.

**Integrity:** Data or information has not been altered or destroyed in an unauthorized manner.

**Involved Persons:** Every employee at ACTION REVENUE RECOVERY, LLC -- no matter what their status. This includes physicians, residents, students, employees, contractors, consultants, temporaries, volunteers, interns, etc.

**Involved Systems:** All computer equipment and network systems that are operated within the ACTION REVENUE RECOVERY, LLC environment. This includes all platforms (operating systems), all computer sizes (personal digital assistants, desktops, mainframes, etc.), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems.

**Protected Health Information (PHI):** PHI is health information, including demographic information, created or received by the ACTION REVENUE RECOVERY, LLC entities which relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an

individual; or the past, present, or future payment for the provision of health care to an individual and that identifies or can be used to identify the individual.

Risk: The probability of a loss of confidentiality, integrity, or availability of information resources.

## V. INFORMATION SECURITY RESPONSIBILITIES

A. Information Security Officer: The Information Security Officer (ISO) for each entity is responsible for working with user management, owners, custodians, and users to develop and implement prudent security policies, procedures, and controls, subject to the approval of ACTION REVENUE RECOVERY, LLC. Specific responsibilities include:

1. Ensuring security policies, procedures, and standards are in place and adhered to by entity.
2. Providing basic security support for all systems and users.
3. Advising owners in the identification and classification of computer resources. See Section VI Information Classification.
4. Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation.
5. Educating custodian and user management with comprehensive information about security controls affecting system users and application systems.
6. Providing on-going employee security education.
7. Performing security audits.
8. Reporting regularly to the ARR's Privacy Department on entity's status with regard to information security.

B. Information Owner: The owner of a collection of information is usually the manager responsible for the creation of that information or the primary user of that information. This role often corresponds with the management of an organizational unit. In this context, ownership does not signify proprietary interest, and ownership may be shared. The owner may delegate ownership responsibilities to another individual by completing the ACTION REVENUE RECOVERY, LLC Information Owner Delegation Form. The owner of information has the responsibility for:

1. Knowing the information for which she/he is responsible.
2. Determining a data retention period for the information, relying on advice from a Legal Source.
3. Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created within the unit.

4. Authorizing access and assigning custodianship.
5. Specifying controls and communicating the control requirements to the custodian and users of the information.
6. Reporting promptly to the ISO the loss or misuse of ACTION REVENUE RECOVERY, LLC information.
7. Initiating corrective actions when problems are identified.
8. Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
9. Following existing approval processes within the respective organizational unit for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

C. Custodian: The custodian of information is generally responsible for the processing and storage of the information. The custodian is responsible for the administration of controls as specified by the owner. Responsibilities may include:

1. Providing and/or recommending physical safeguards.
2. Providing and/or recommending procedural safeguards.
3. Administering access to information.
4. Releasing information as authorized by the Information Owner and/or the Information Privacy/ Security Officer for use and disclosure using procedures that protect the privacy of the information.
5. Evaluating the cost effectiveness of controls.
6. Maintaining information security policies, procedures and standards as appropriate and in consultation with the ISO.
7. Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
8. Reporting promptly to the ISO the loss or misuse of ACTION REVENUE RECOVERY, LLC information.
9. Identifying and responding to security incidents and initiating appropriate actions when problems are identified.

D. User Management: ACTION REVENUE RECOVERY, LLC management who supervise users as defined below. User management is responsible for overseeing their employees' use of information, including:

1. Reviewing and approving all requests for their employee's access authorizations.
2. Initiating security change requests to keep employees' security record current with their positions and job functions.

3. Promptly informing appropriate parties of employee terminations and transfers, in accordance with local entity termination procedures.

4. Revoking physical access to terminated employees, i.e., confiscating keys, changing combination locks, etc.

5. Providing employees with the opportunity for training needed to properly use the computer systems.

6. Reporting promptly to the ISO the loss or misuse of ACTION REVENUE RECOVERY, LLC information.

7. Initiating corrective actions when problems are identified.

8. Following existing approval processes within their respective organization for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

E. User: The user is any person who has been authorized to read, enter, or update information. A user of information is expected to:

1. Access information only in support of their authorized job responsibilities.

2. Comply with Information Security Policies and Standards and with all controls established by the owner and custodian.

3. Refer all disclosures of PHI (1) outside of ACTION REVENUE RECOVERY, LLC and (2) within ACTION REVENUE RECOVERY, LLC, other than for treatment, payment, or health care operations, to the applicable entity's Medical/Health Information Management Department. In certain circumstances, the Medical/Health Information Management Department policies may specifically delegate the disclosure process to other departments.

4. Keep personal authentication devices (e.g. passwords, Secure Cards, PINs, etc.) confidential.

5. Report promptly to the ISO the loss or misuse of ACTION REVENUE RECOVERY, LLC information.

6. Initiate corrective actions when problems are identified.

## VI. INFORMATION CLASSIFICATION

Classification is used to promote proper controls for safeguarding the confidentiality of information. Regardless of classification the integrity and accuracy of all classifications of information must be protected. The classification assigned and the related controls applied are dependent on the sensitivity of the information. Information must be classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, report) must have the same classification regardless of format. The following levels are to be used when classifying information:

#### A. Protected Health Information (PHI)

1. PHI is information, whether oral or recorded in any form or medium, that: a. is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university or health clearinghouse; and b. relates to past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past present or future payment for the provision of health care to an individual; and c. includes demographic data, that permits identification of the individual or could reasonably be used to identify the individual.
2. Unauthorized or improper disclosure, modification, or destruction of this information could violate state and federal laws, result in civil and criminal penalties, and cause serious damage to ACTION REVENUE RECOVERY, LLC, its clients and their patients.

#### B. Confidential Information

1. Confidential Information is very important and highly sensitive material that is not classified as PHI. This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. Examples of Confidential Information may include: personnel information, key financial information, system access passwords and information file encryption keys.
2. Unauthorized disclosure of this information to people without a business need for access may violate laws and regulations, or may cause significant problems for ACTION REVENUE RECOVERY, LLC, its clients, or its business partners. Decisions about the provision of access to this information must always be cleared through the information owner.

#### C. Internal Information

1. Internal Information is intended for unrestricted use within ACTION REVENUE RECOVERY, LLC, and in some cases within affiliated organizations such as ACTION REVENUE RECOVERY, LLC business partners. This type of information is already widely-distributed within ACTION REVENUE RECOVERY, LLC, or it could be so distributed within the organization without advance permission from the information owner. Examples of Internal Information may include: personnel directories, internal policies and procedures, most internal electronic mail messages.
2. Any information not explicitly classified as PHI, Confidential or Public will, by default, be classified as Internal Information.
3. Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions.

#### D. Public Information

1. Public Information has been specifically approved for public release by a designated authority within each entity of ACTION REVENUE RECOVERY, LLC. Examples of Public Information may include marketing brochures and material posted to ACTION REVENUE RECOVERY, LLC entity internet web pages.
2. This information may be disclosed outside of ACTION REVENUE RECOVERY, LLC.

#### VII. COMPUTER AND INFORMATION CONTROL

All involved systems and information are assets of ACTION REVENUE RECOVERY, LLC and are expected to be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

##### A. Ownership of Software:

All computer software developed by ACTION REVENUE RECOVERY, LLC employees or contract personnel on behalf of ACTION REVENUE RECOVERY, LLC or licensed for ACTION REVENUE RECOVERY, LLC use is the property of ACTION REVENUE RECOVERY, LLC and must not be copied for use at home or any other location, unless otherwise specified by the license agreement.

##### B. Installed Software:

All software packages that reside on computers and networks within ACTION REVENUE RECOVERY, LLC must comply with applicable licensing agreements and restrictions and must comply with ACTION REVENUE RECOVERY, LLC acquisition of software policies.

##### C. Virus Protection:

Virus checking systems approved by the Information Security Officer and Information Services must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses. Users are not authorized to turn off or disable virus checking systems.

##### D. Access Controls:

Physical and electronic access to PHI, Confidential and Internal information and computing resources is controlled. To ensure appropriate levels of access by internal workers, a variety of security measures will be instituted as recommended by the Information Security Officer and approved by ACTION REVENUE RECOVERY, LLC. Mechanisms to control access to PHI, Confidential and Internal information include (but are not limited to) the following methods:

1. Authorization: Access will be granted on a "need to know" basis and must be authorized by the immediate supervisor and application owner with the assistance of the ISO. Any of the following methods are acceptable for providing access under this policy:

a. Context-based access: Access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The “external” factors might include time of day, location of the user, strength of user authentication, etc.

b. Role-based access: An alternative to traditional access control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization’s structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.

c. User-based access: A security mechanism used to grant users of a system access based upon the identity of the user.

2. Identification/Authentication: Unique user identification (user id) and authentication is required for all systems that maintain or access PHI, Confidential and/or Internal Information. Users will be held accountable for all actions performed on the system with their user id.

a. At least one of the following authentication methods must be implemented:

1. Strictly controlled passwords,
2. Biometric identification, and/or
3. Tokens in conjunction with a PIN.

b. The user must secure his/her authentication control (e.g. password, token) such that it is known only to that user and possibly a designated security manager.

c. An automatic timeout re-authentication must be required after a certain period of no activity (5 minutes).

d. The user must log off or secure the system when leaving it.

3. Data Integrity: ACTION REVENUE RECOVERY, LLC must be able to provide corroboration that PHI, Confidential, and Internal Information has not been altered or destroyed in an unauthorized manner. Listed below are some methods that support data integrity:

- a. transaction audit
- b. disk redundancy (RAID)
- c. ECC (Error Correcting Memory)
- d. checksums (file integrity)
- e. encryption of data in storage
- f. digital signatures

4. Transmission Security: Technical security mechanisms must be put in place to guard against unauthorized access to data that is transmitted over a communications network, including wireless networks. The following features must be implemented:

- a. integrity controls and

b. encryption, where deemed appropriate

5. Remote Access: Access into ACTION REVENUE RECOVERY, LLC network from outside will be granted using ACTION REVENUE RECOVERY, LLC approved devices and pathways on an individual user and application basis. All other network access options are strictly prohibited. Further, PHI, Confidential and/or Internal Information that is stored or accessed remotely must maintain the same level of protections as information stored and accessed within the ACTION REVENUE RECOVERY, LLC network.

6. Physical Access: Access to areas in which information processing is carried out must be restricted to only appropriately authorized individuals. The following physical controls must be in place:

a. Mainframe computer systems must be installed in an access-controlled area. The area in and around the computer facility must afford protection against water damage, and other environmental hazards such as power outages and extreme temperature situations.

b. File servers containing PHI, Confidential and/or Internal Information must be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.

c. Workstations or personal computers (PC) must be secured against use by unauthorized individuals. Local procedures and standards must be developed on secure and appropriate workstation use and physical safeguards which must include procedures that will:

1. Position workstations to minimize unauthorized viewing of protected health information.

2. Grant workstation access only to those who need it in order to perform their job function.

3. Establish workstation location criteria to eliminate or minimize the possibility of unauthorized access to protected health information.

4. Employ physical safeguards as determined by risk analysis, such as locating workstations in controlled access areas or installing covers or enclosures to preclude passerby access to PHI.

5. Use automatic screen savers with passwords to protect unattended machines.

d. Facility access controls must be implemented to limit physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed. Local policies and procedures must be developed to address the following facility access control requirements:

1. Contingency Operations: Documented procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

2. Facility Security Plan: Documented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

3. Access Control and Validation: Documented procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

4. Maintenance records: Documented policies and procedures to document repairs and modifications to the physical components of the facility which are related to security (for example, hardware, walls, doors, and locks).

7. Emergency Access:

a. Each entity is required to establish a mechanism to provide emergency access to systems and applications in the event that the assigned custodian or owner is unavailable during an emergency.

b. Procedures must be documented to address:

1. Authorization,
2. Implementation, and
3. Revocation

E. Equipment and Media Controls: The disposal of information must ensure the continued protection of PHI, Confidential and Internal Information. Each entity must develop and implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain PHI into and out of a facility, and the movement of these items within the facility. The following specification must be addressed:

1. Information Disposal / Media Re-Use of:

- a. Hard copy (paper and microfilm/fiche)
- b. Magnetic media (floppy disks, hard drives, zip disks, etc.) and
- c. CD ROM Disks

2. Accountability: Each entity must maintain a record of the movements of hardware and electronic media and any person responsible therefore.

3. Data backup and Storage: When needed, create a retrievable, exact copy of electronic PHI before movement of equipment.

F. Other Media Controls:

1. PHI and Confidential Information stored on external media (diskettes, cd-roms, portable storage, memory sticks, etc.) must be protected from theft and unauthorized access. Such media must be appropriately labeled so as to identify it as PHI or Confidential Information. Further, external media containing PHI and Confidential Information must never be left unattended in unsecured areas.

2. PHI and Confidential Information must never be stored on mobile computing devices (laptops, personal digital assistants (PDA), smart phones, tablet PC's, etc.) unless the devices have the following minimum security requirements implemented:

- a. Power-on passwords
  - b. Auto logoff or screen saver with password
  - c. Encryption of stored data or other acceptable safeguards approved by Information Security Officer
- Further, mobile computing devices must never be left unattended in unsecured areas.

3. If PHI or Confidential Information is stored on external medium or mobile computing devices and there is a breach of confidentiality as a result, then the owner of the medium/device will be held personally accountable and is subject to the terms and conditions of ACTION REVENUE RECOVERY, LLC Information Security Policies and Confidentiality Statement signed as a condition of employment or affiliation with ACTION REVENUE RECOVERY, LLC.

H. Data Transfer/Printing:

1. Electronic Mass Data Transfers: Downloading and uploading PHI, Confidential, and Internal Information between systems must be strictly controlled. Requests for mass download of, or individual requests for, information for research purposes that include PHI must be approved through the Internal Review Board (IRB). All other mass downloads of information must be approved by the Application Owner and include only the minimum amount of information necessary to fulfill the request. Applicable Business Associate Agreements must be in place when transferring PHI to external entities.

2. Other Electronic Data Transfers and Printing: PHI, Confidential and Internal Information must be stored in a manner inaccessible to unauthorized individuals. PHI and Confidential information must not be downloaded, copied or printed indiscriminately or left unattended and open to compromise. PHI that is downloaded for educational purposes where possible should be de-identified before use.

I. Oral Communications: ACTION REVENUE RECOVERY, LLC staff should be aware of their surroundings when discussing PHI and Confidential Information. This includes the use of cellular telephones in public areas. ACTION REVENUE RECOVERY, LLC staff should not discuss PHI or Confidential Information in public areas if the information can be overheard. Caution should be used when conducting conversations in: waiting areas, break rooms, corridors, elevators, parking areas, restaurants, or on public transportation.

J. Audit Controls: Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use PHI must be implemented. Further, procedures must be implemented to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. These reviews must be documented and maintained for six (6) years.

K. Evaluation: ACTION REVENUE RECOVERY, LLC requires that periodic technical and non-technical evaluations be performed in response to environmental or operational changes affecting the security of electronic PHI to ensure its continued protection.

L. Contingency Plan: Controls must ensure that ACTION REVENUE RECOVERY, LLC can recover from any damage to computer equipment or files within a reasonable period of time. Each entity is required to develop and maintain a plan for responding to a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems that contain PHI, Confidential, or Internal Information. This will include developing policies and procedures to address the following:

1. Data Backup Plan:

- a. A data backup plan must be documented and routinely updated to create and maintain, for a specific period of time, retrievable exact copies of information.
- b. Backup data must be stored in an off-site location and protected from physical damage.
- c. Backup data must be afforded the same level of protection as the original data.

2. Disaster Recovery Plan: A disaster recovery plan must be developed and documented which contains a process enabling the entity to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.

3. Emergency Mode Operation Plan: A plan must be developed and documented which contains a process enabling the entity to continue to operate in the event of fire, vandalism, natural disaster, or system failure.

4. Testing and Revision Procedures: Procedures should be developed and documented requiring periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary.

5. Applications and Data Criticality Analysis: The criticality of specific applications and data in support of other contingency plan components must be assessed and documented.

Compliance [§ 164.308(a)(1)(ii)(C)]

A. The Information Security Policy applies to all users of ACTION REVENUE RECOVERY, LLC information including: employees and outside affiliates. Failure to comply with Information Security Policies and Standards by employees and outside affiliates may result in disciplinary action up to and including dismissal in accordance with applicable ACTION REVENUE RECOVERY, LLC procedures, or, in the case of outside affiliates, termination of the affiliation. Further, penalties associated with state and federal laws may apply.

B. Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:

1. Unauthorized disclosure of PHI or Confidential Information as specified in Confidentiality Statement.
2. Unauthorized disclosure of a sign-on code (user id) or password.
3. Attempting to obtain a sign-on code or password that belongs to another person.
4. Using or attempting to use another person's sign-on code or password.
5. Unauthorized use of an authorized password to invade patient privacy by examining records or information for which there has been no request for review.
6. Installing or using unlicensed software on ACTION REVENUE RECOVERY, LLC computers.
7. The intentional unauthorized destruction of ACTION REVENUE RECOVERY, LLC information.
8. Attempting to get access to sign-on codes for purposes other than official business, including completing fraudulent documentation to gain access.

## Password Control Standards

The ACTION REVENUE RECOVERY, LLC Information Security Policy requires the use of strictly controlled passwords for accessing Protected Health Information (PHI), Confidential Information (CI) and Internal Information (II). (See ACTION REVENUE RECOVERY, LLC Information Security Policy for definition of these protected classes of information.) Listed below are the minimum standards that must be implemented in order to ensure the effectiveness of password controls.

Standards for accessing PHI, CI, II:

Users are responsible for complying with the following password standards:

1. Passwords must never be shared with another person, unless the person is a designated security manager.
2. Every password must, where possible, be changed regularly (between 45 and 90 days depending on the sensitivity of the information being accessed)
3. Passwords must, where possible, have a minimum length of six characters.
4. Passwords must never be saved when prompted by any application with the exception of central single sign-on (SSO) systems as approved by the ISO. This feature should be disabled in all applicable systems.
5. Passwords must not be programmed into a PC or recorded anywhere that someone may find and use them.
6. When creating a password, it is important not to use words that can be found in dictionaries or words that are easily guessed due to their association with the user (i.e. children's names, pets' names, birthdays, etc...). A combination of alpha and numeric characters is more difficult to guess. Where possible, system software must enforce the following password standards:

1. Passwords routed over a network must be encrypted.
2. Passwords must be entered in a non-display field.
3. System software must enforce the changing of passwords and the minimum length.
4. System software must disable the user identification code when more than three consecutive invalid passwords are given within a 15 minute timeframe. Lockout time must be set at a minimum of 30 minutes.
5. System software must maintain a history of previous passwords and prevent their reuse.



**ACTION REVENUE RECOVERY, LLC**  
**Policy on Confidentiality and Dissemination of Patient**  
**Information and Staff Member Verification**

Given the nature of our work, it is imperative that we maintain the confidence of patient/client information that we receive in the course of our work. ACTION REVENUE RECOVERY, LLC prohibits the release of any patient/client information to anyone outside the department except in limited circumstances and discussions or disclosures of protected health information (PHI) within the organization should be limited to the minimum necessary that is needed for the recipient of the information to perform their job. Acceptable uses of PHI within the organization include but are not limited to peer review, internal audits, quality assurance and billing/collections. I understand ACTION REVENUE RECOVERY, LLC provides services to patient/clients that are private and confidential and that I am a crucial step in respecting the privacy rights of ACTION REVENUE RECOVERY, LLC patients/clients. I understand that it is necessary, in the rendering of ACTION REVENUE RECOVERY, LLC services, that patients/clients provide personal information and that such information may exist in a variety of forms such as electronic, oral, written or photographic and that all such information is strictly confidential and protected by federal and state laws that prohibit its unauthorized use or disclosure. I have received training in the confidentiality policies and procedures set in place by ACTION RECOVERY, LLC and agree I will comply with such policies and procedures during my entire employment with ACTION REVENUE RECOVERY, LLC. If I, at any time, knowingly or inadvertently breach the patient/client confidentiality policies and procedures, I agree to notify the ACTION REVENUE RECOVERY, LLC HIPAA Privacy Officer Liaison immediately. In addition, I understand that breach of patient/client confidentiality or privacy may result in disciplinary action up to and including suspension or termination of my employment with ACTION REVENUE RECOVERY, LLC. Upon separation of my employment for any reason, or at any time upon request, I agree to return any and all patient/client confidential information in my possession.

I have read and understand all privacy policies and procedures that have been provided to me by ACTION REVENUE RECOVERY, LLC. I agree to all conditions of my employment set forth in this agreement. This is not a contract of employment and does not alter the nature of the at-will employment relationship between ACTION REVENUE RECOVERY, LLC and me.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Policies and Procedures  
HIPAA Policy on PHI Access/Security

**ACTION REVENUE RECOVERY, LLC Policy on Security, Levels of Access and Limiting  
Disclosure and Use of Protected Health Information**



## **BUSINESS ASSOCIATE AGREEMENT**

This Business Associate Agreement (“Agreement”), dated \_\_\_\_\_, 20\_\_\_\_, is entered into by Action Revenue Recovery, LLC (“Covered Entity”) and \_\_\_\_\_ (the “Business Associate”) (each a “Party” and collectively the “Parties”), and is made a part of that certain service agreement or service agreements between the parties (the “Service Agreement”) pursuant to which Business Associate provides a service or services to Covered Entity that involves the use and/or disclosure of Covered Entity’s Protected Health Information (“PHI”).

NOW, THEREFORE, for good and valuable consideration, the sufficiency of which we hereby acknowledge, the Parties agree as follows:

### **I. DEFINITIONS:**

- A. Terms used but not otherwise defined in this Agreement shall have the same meaning as the meaning ascribed to those terms in the Health Information Portability and Accountability Act of 1996, as codified at 42 U.S.C. § 1320d (“HIPAA”), the Health Information Technology Act of 2009, as codified at 42 U.S.C.A. prec. § 17901 (“HITECH Act”), and any current and future regulations promulgated under HIPAA or the HITECH Act (HIPAA, HITECH Act and any current and future regulations promulgated under either are referred to as the “Regulations”).
  
- B. *Protected Health Information or PHI.* “Protected Health Information” or “PHI” shall have the same meaning as the term “Protected Health Information” in 45 CFR 160.103, limited to the information

created or received by Business Associate from or on behalf of Covered Entity, including, but not limited to electronic PHI.

## **II. OBLIGATIONS OF BUSINESS ASSOCIATE**

In order that Covered Entity and Business Associate may achieve and maintain compliance with the requirements of HIPAA, Business Associate agrees:

- A. To only use and disclose PHI as permitted by this Agreement or as Required By Law. Business Associate may 1) use and disclose PHI to perform its obligations as set forth in the Service Agreement; (2) use PHI for the proper management and administration of Business Associate or to carry out its legal responsibilities; (3) disclose PHI for the proper management and administration of Business Associate or to carry out its legal responsibilities, if such disclosure is required by law or if Business Associate obtains reasonable assurances from the recipient that the recipient will keep the PHI confidential, use or further disclose the PHI only as required by law or for the purpose for which it was disclosed to the recipient, and notify Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached; (4) use PHI to provide data aggregation services relating to the health care operations of Covered Entity; (5) use or disclose PHI to report violations of the law to law enforcement; and (6) use PHI to create de-identified information consistent with the standards set forth at 45 CFR § 164.514. Business Associate will not sell PHI or use or disclose PHI for purposes of marketing, as defined and proscribed in the Regulations.
  
- B. To limit its uses and disclosures of, and requests for, PHI (a) when practical, to the information making up a Limited Data Set; and (b) in all other cases subject to the requirements of 45 CFR 164.502(b), to the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request;
  
- C. To use appropriate administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of the PHI in compliance with the Regulations.

- D. To require all of its subcontractors and agents that receive, use or have access to PHI to agree, in writing, to adhere to the same restrictions and conditions on the use or disclosure of PHI that apply to the Business Associate pursuant to this Agreement;
- E. Upon reasonable notice and prior written request, to make available during normal business hours at Business Associate's offices all records, books, agreements, internal practices, policies and procedures relating to the use or disclosure of PHI to the Secretary, in a time and manner designated by the Secretary, for purposes of determining the Covered Entity's compliance with the Regulations, subject to attorney-client and other applicable legal privileges;
- F. To provide documentation regarding any disclosures by Business Associate that would have to be included in an accounting of disclosures to an Individual under 45 CFR 164.528 (including without limitation a disclosure permitted under 45 CFR 164.512) and the HITECH Act, within a reasonable amount of time of receipt of a request from Covered Entity;
- G. If, and to the extent that Business Associate possesses an applicable Designated Record Set, within a reasonable amount of time of receipt of a request from the Covered Entity for the amendment of an individual's PHI contained in the Designated Record Set, Business Associate shall provide such information to the Covered Entity for amendment and shall also incorporate any such amendments in the PHI maintained by Business Associate as required by 45 C.F.R. 164.526.
- H. Subject to Section III.C.2. of this Agreement, return to the Covered Entity or destroy, within thirty (30) days of the termination of this Agreement, any and all PHI in its possession and retain no copies (which for purposes of this Agreement shall include without limitation destroying all backup tapes and permanently deleting all electronic PHI).

- I. To mitigate, to the extent practicable, any harmful effects from any use or disclosure of PHI by Business Associate not permitted by this Agreement.
  
- J. Business Associate agrees to notify the designated Privacy Official of the Covered Entity of any use or disclosure of PHI by Business Associate not permitted by this Agreement, any Security Incident involving electronic PHI, and any Breach of Unsecured Protected Health Information within five (5) business days.
  - 1. Business Associate shall provide the following information to Covered Entity within ten (10) business days of discovery of a breach except when despite all reasonable efforts by Business Associate to obtain the information required, circumstances beyond the control of the Business Associate necessitate additional time. Under such circumstances Business Associate shall provide to Covered Entity the following information as soon as possible and without unreasonable delay, but in no event later than thirty (30) calendar days from the date of discovery of a breach:
    - a. the date of the breach;
    - b. the date of the discovery of the breach;
    - c. a description of the types of unsecured PHI that were involved;
    - d. identification of each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed; and
    - e. any other details necessary to complete an assessment of the risk of harm to the individual.
  - 2. Covered Entity will be responsible to provide notification to individuals whose unsecured PHI has been disclosed, as well as the Secretary and the media, as required by Sec. 13402 of the HITECH Act, 42 U.S.C.A. § 17932;
  - 3. Business associate agrees to pay actual costs for notification and of any associated mitigation incurred by Covered Entity, such as credit monitoring, if Covered Entity determines that the breach is significant enough to warrant such measures.
  - 4. Business associate agrees to establish procedures to investigate the breach, mitigate losses, and protect against any future breaches, and to provide a description of these procedures and the specific findings of the investigation to Covered Entity in the time and manner reasonably requested by Covered Entity.

5. The parties agree that this section satisfies any notices necessary by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional notice to Covered Entity shall be required. For purposes of this Agreement, "Unsuccessful Security Incidents" include activity such as pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of electronic PHI.

### **III. TERM AND TERMINATION:**

- A. Term. This Agreement shall become effective on the date of execution of a Service Agreement, and shall terminate upon the termination or expiration of all Service Agreement(s). Notwithstanding the foregoing, obligations imposed on either party pursuant to the HITECH Act must be complied with only when the particular provisions referenced become effective or compliance becomes required, whichever is later.
- B. Termination for Cause. Either Party may immediately terminate this Agreement and the Service Agreement(s) if such Party makes the determination that the other Party has breached a material term of this Agreement. Alternatively, the terminating Party may choose to provide the other Party with thirty (30) days written notice of the existence of an alleged material breach and an opportunity to cure the breach. If termination is not feasible, the terminating Party shall report the breach to the Secretary.
- C. Effect of Termination.
  1. Upon termination or expiration of this Agreement, Business Associate agrees to return to Covered Entity or destroy all PHI in the possession of Business Associate and/or in the possession of any subcontractor or agent of Business Associate and to retain no copies of the PHI.

2. In the event that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity a written statement that it is infeasible to return or destroy the PHI and describe the conditions that make return or destruction of the PHI infeasible. Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains the PHI.

#### **IV. MISCELLANEOUS:**

- A. Amendments. This Agreement may not be modified, nor shall any provision hereof be waived or amended, except in a writing duly signed by authorized representatives of the Parties. The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary to achieve and maintain compliance with the requirements of the Regulations.
- B. Regulatory References. Any reference herein to a federal regulatory section within the Code of Federal Regulations shall be a reference to such section as it may be subsequently updated, amended or modified.
- C. Interpretation. Any ambiguity in this Agreement shall be resolved to permit covered entities to comply with HIPAA.
- D. Notices. Any notices hereunder shall be in writing and addressed as follows:

If to the Covered Entity:

Action Revenue Recovery, LLC

910 Bres Avenue

Monroe, LA 71201

Attention: Drew Kennedy, CEO

If to Business Associate:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Attention: \_\_\_\_\_

IN WITNESS WHEREOF, each of the undersigned has caused this Agreement to be executed by its duly authorized representative.

FOR ACTION REVENUE RECOVERY, LLC

Name: \_\_\_\_\_

\_\_\_\_\_ Date

Title: \_\_\_\_\_

FOR BUSINESS ASSOCIATE

Name: \_\_\_\_\_

\_\_\_\_\_ Date

Title: \_\_\_\_\_



## **BUSINESS ASSOCIATE AGREEMENT**

This Business Associate Agreement (“Agreement”), dated \_\_\_\_\_, 20\_\_\_\_, is entered into by Action Revenue Recovery, LLC (“Business Associate”) and \_\_\_\_\_ (the “Covered Entity”) (each a “Party” and collectively the “Parties”), and is made a part of that certain service agreement or service agreements between the parties (the “Service Agreement”) pursuant to which Business Associate provides a service or services to Covered Entity that involves the use and/or disclosure of Covered Entity’s Protected Health Information (“PHI”).

NOW, THEREFORE, for good and valuable consideration, the sufficiency of which we hereby acknowledge, the Parties agree as follows:

### **V. DEFINITIONS:**

- A. Terms used but not otherwise defined in this Agreement shall have the same meaning as the meaning ascribed to those terms in the Health Information Portability and Accountability Act of 1996, as codified at 42 U.S.C. § 1320d (“HIPAA”), the Health Information Technology Act of 2009, as codified at 42 U.S.C.A. prec. § 17901 (“HITECH Act”), and any current and future regulations promulgated under HIPAA or the HITECH Act (HIPAA, HITECH Act and any current and future regulations promulgated under either are referred to as the “Regulations”).
- B. *Protected Health Information or PHI.* “Protected Health Information” or “PHI” shall have the same meaning as the term “Protected Health Information” in 45 CFR 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity, including, but not limited to electronic PHI.

## VI. OBLIGATIONS OF BUSINESS ASSOCIATE

In order that Covered Entity and Business Associate may achieve and maintain compliance with the requirements of HIPAA, Business Associate agrees:

- A. To only use and disclose PHI as permitted by this Agreement or as Required By Law. Business Associate may 1) use and disclose PHI to perform its obligations as set forth in the Service Agreement; (2) use PHI for the proper management and administration of Business Associate or to carry out its legal responsibilities; (3) disclose PHI for the proper management and administration of Business Associate or to carry out its legal responsibilities, if such disclosure is required by law or if Business Associate obtains reasonable assurances from the recipient that the recipient will keep the PHI confidential, use or further disclose the PHI only as required by law or for the purpose for which it was disclosed to the recipient, and notify Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached; (4) use PHI to provide data aggregation services relating to the health care operations of Covered Entity; (5) use or disclose PHI to report violations of the law to law enforcement; and (6) use PHI to create de-identified information consistent with the standards set forth at 45 CFR § 164.514. Business Associate will not sell PHI or use or disclose PHI for purposes of marketing, as defined and proscribed in the Regulations.
- B. To limit its uses and disclosures of, and requests for, PHI (a) when practical, to the information making up a Limited Data Set; and (b) in all other cases subject to the requirements of 45 CFR 164.502(b), to the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request;
- C. To use appropriate administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of the PHI in compliance with the Regulations.
- D. To require all of its subcontractors and agents that receive, use or have access to PHI to agree, in writing, to adhere to the same

restrictions and conditions on the use or disclosure of PHI that apply to the Business Associate pursuant to this Agreement;

- E. Upon reasonable notice and prior written request, to make available during normal business hours at Business Associate's offices all records, books, agreements, internal practices, policies and procedures relating to the use or disclosure of PHI to the Secretary, in a time and manner designated by the Secretary, for purposes of determining the Covered Entity's compliance with the Regulations, subject to attorney-client and other applicable legal privileges;
- F. To provide documentation regarding any disclosures by Business Associate that would have to be included in an accounting of disclosures to an Individual under 45 CFR 164.528 (including without limitation a disclosure permitted under 45 CFR 164.512) and the HITECH Act, within a reasonable amount of time of receipt of a request from Covered Entity;
- G. If, and to the extent that Business Associate possesses an applicable Designated Record Set, within a reasonable amount of time of receipt of a request from the Covered Entity for the amendment of an individual's PHI contained in the Designated Record Set, Business Associate shall provide such information to the Covered Entity for amendment and shall also incorporate any such amendments in the PHI maintained by Business Associate as required by 45 C.F.R. 164.526.
- H. Subject to Section III.C.2. of this Agreement, return to the Covered Entity or destroy, within thirty (30) days of the termination of this Agreement, any and all PHI in its possession and retain no copies (which for purposes of this Agreement shall include without limitation destroying all backup tapes and permanently deleting all electronic PHI).
- I. To mitigate, to the extent practicable, any harmful effects from any use or disclosure of PHI by Business Associate not permitted by this Agreement.

- J. Business Associate agrees to notify the designated Privacy Official of the Covered Entity of any use or disclosure of PHI by Business Associate not permitted by this Agreement, any Security Incident involving electronic PHI, and any Breach of Unsecured Protected Health Information within five (5) business days.
6. Business Associate shall provide the following information to Covered Entity within ten (10) business days of discovery of a breach except when despite all reasonable efforts by Business Associate to obtain the information required, circumstances beyond the control of the Business Associate necessitate additional time. Under such circumstances Business Associate shall provide to Covered Entity the following information as soon as possible and without unreasonable delay, but in no event later than thirty (30) calendar days from the date of discovery of a breach:
    - a. the date of the breach;
    - b. the date of the discovery of the breach;
    - c. a description of the types of unsecured PHI that were involved;
    - d. identification of each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed; and
    - e. any other details necessary to complete an assessment of the risk of harm to the individual.
  7. Covered Entity will be responsible to provide notification to individuals whose unsecured PHI has been disclosed, as well as the Secretary and the media, as required by Sec. 13402 of the HITECH Act, 42 U.S.C.A. § 17932;
  8. Business associate agrees to pay actual costs for notification and of any associated mitigation incurred by Covered Entity, such as credit monitoring, if Covered Entity determines that the breach is significant enough to warrant such measures.
  9. Business associate agrees to establish procedures to investigate the breach, mitigate losses, and protect against any future breaches, and to provide a description of these procedures and the specific findings of the investigation to Covered Entity in the time and manner reasonably requested by Covered Entity.
  10. The parties agree that this section satisfies any notices necessary by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional notice to Covered Entity shall be required. For

purposes of this Agreement, "Unsuccessful Security Incidents" include activity such as pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of electronic PHI.

## **VII. TERM AND TERMINATION:**

- A. Term. This Agreement shall become effective on the date of execution of a Service Agreement, and shall terminate upon the termination or expiration of all Service Agreement(s). Notwithstanding the foregoing, obligations imposed on either party pursuant to the HITECH Act must be complied with only when the particular provisions referenced become effective or compliance becomes required, whichever is later.
- B. Termination for Cause. Either Party may immediately terminate this Agreement and the Service Agreement(s) if such Party makes the determination that the other Party has breached a material term of this Agreement. Alternatively, the terminating Party may choose to provide the other Party with thirty (30) days written notice of the existence of an alleged material breach and an opportunity to cure the breach. If termination is not feasible, the terminating Party shall report the breach to the Secretary.
- C. Effect of Termination.
1. Upon termination or expiration of this Agreement, Business Associate agrees to return to Covered Entity or destroy all PHI in the possession of Business Associate and/or in the possession of any subcontractor or agent of Business Associate and to retain no copies of the PHI.
  2. In the event that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity a written statement that it is infeasible to return or destroy the PHI and describe the conditions that make return or destruction of the

PHI infeasible. Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains the PHI.

#### **VIII. MISCELLANEOUS:**

- A. Amendments. This Agreement may not be modified, nor shall any provision hereof be waived or amended, except in a writing duly signed by authorized representatives of the Parties. The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary to achieve and maintain compliance with the requirements of the Regulations.
  
- B. Regulatory References. Any reference herein to a federal regulatory section within the Code of Federal Regulations shall be a reference to such section as it may be subsequently updated, amended or modified.
  
- C. Interpretation. Any ambiguity in this Agreement shall be resolved to permit covered entities to comply with HIPAA.
  
- D. Notices. Any notices hereunder shall be in writing and addressed as follows:

If to the Business Associate:

Action Revenue Recovery, LLC

910 Bres Avenue

Monroe, LA 71201

Attention: Drew Kennedy, CEO

If to Covered Entity:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Attention: \_\_\_\_\_

IN WITNESS WHEREOF, each of the undersigned has caused this Agreement to be executed by its duly authorized representative.

FOR ACTION REVENUE RECOVERY, LLC

Name: \_\_\_\_\_

\_\_\_\_\_ Date

Title: \_\_\_\_\_

FOR COVERED ENTITY

Name: \_\_\_\_\_

\_\_\_\_\_ Date

Title: \_\_\_\_\_

## **PRIVACY BREACH NOTIFICATION FORM FOR THE SECRETARY OF HHS**

The breach notification provisions of section 13402(h) of the HITECH Act apply to HIPAA covered entities and their business associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured PHI.

In the event of a privacy breach, the link below is an online form that Action Revenue Recovery, LLC will use to submit the details of the disclosure directly to the Secretary of Health and Human Services.

<http://transparency.cit.nih.gov/breach/index.cfm>