Business Associate Agreement

In order to comply with the requirements of the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), such Acts implementing regulations, and, if applicable, the federal drug and alcohol treatment privacy regulations at 42 C.F.R. Part 2, this Business Associate Agreement ("Agreement") is hereby entered into between _____ ("COMPANY") and _____ ("BUSINESS ASSOCIATE").

1. Purpose and Scope. The purposes of this Agreement are to (1) establish the permitted and required uses and disclosures by BUSINESS ASSOCIATE of protected health information and electronic protected health information (collectively referred to as PHI) it may possess by reason of this contract and (2) provide BUSINESS ASSOCIATE with Company's Code of Compliance and Ethical Standards. This Agreement does not apply to disclosures by another covered entity regarding treatment of an individual. BUSINESS ASSOCIATE specifically agrees:

- BUSINESS ASSOCIATE will comply with Company's policies and procedures as well as it own, and all applicable laws regarding the use or disclosure of PHI as they relate to this contract;
- BUSINESS ASSOCIATE may use and disclose PHI as necessary for the proper management and administration of BUSINESS ASSOCIATE or to carry out the legal responsibilities of BUSINESS ASSOCIATE; provided that, if any such disclosure is to a third party, the disclosure will be made pursuant to this Agreement.

2. Uses and Disclosures. Except as required by law or authorized by the individual who is the subject of the information, BUSINESS ASSOCIATE will appropriately safeguard PHI in accordance with the provisions of this Agreement, 45 C.F.R. Part 164 and, if applicable, 42 C.F.R. Part 2. BUSINESS ASSOCIATE hereby agrees that BUSINESS ASSOCIATE will:

- not use or further disclose the information other than as required or permitted by law or this contract;
- use appropriate safeguards to prevent use or disclosure of the information other than as provided for herein;
- if applicable, be bound by 42 C.F.R. Part 2 with respect to any PHI received related to Company's alcohol and drug abuse programs;
- report to COMPANY uses or disclosures of the information not provided for by this contract of which it becomes aware;
- ensure that any agents, including a subcontractor, to whom it provides PHI will also agree to the same restrictions contained in this Agreement.
- make the information available to the individual upon written request;
- make the information available for, and will incorporate any, amendments in accordance with 45 C.F.R. Part 164;
- provide an accounting to the individual of uses and disclosures BUSINESS ASSOCIATE has made of such information upon request by the individual;
- if applicable, resist in judicial proceedings, if necessary, any efforts to obtain access to patient records which would (i) identify a patient as an alcohol or drug abuser, or (ii) is drug abuse information obtained by a federally assisted alcohol or drug abuse program, except as permitted by 42 C.F.R. Part 2;
- make available BUSINESS Associate's books and records relating to the uses and disclosures of PHI made pursuant to this contract to the Secretary of DHHS and COMPANY for purposes of determining BUSINESS Associate's compliance with the above privacy/security laws, policies and procedures ;
- upon termination of this contract, return or destroy all PHI created or received on behalf of the COMPANY. Additionally, BUSINESS ASSOCIATE will retain no copies of the PHI. If returning or destroying the information is not feasible, BUSINESS ASSOCIATE will continue to safeguard such information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

3. Electronic Protected Health Information (ePHI). During the term of this Agreement, COMPANY may permit BUSINESS ASSOCIATE to create, receive, maintain or transmit electronic protected health information (ePHI) on Company's behalf. With respect to such ePHI, BUSINESS ASSOCIATE agrees to:

- implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the ePHI; and
- ensure that any agent, including a subcontractor, to whom BUSINESS ASSOCIATE provides such ePHI, agrees to implement reasonable and appropriate safeguards to protect the ePHI.

4. Notification in Case of Breach. BUSINESS ASSOCIATE shall, following the discovery of a breach of unsecured PHI/ePHI, notify COMPANY within 5 business days of such breach. Such notice shall include the identification of each individual whose unsecured PHI/ePHI has been, or is reasonably believed by BUSINESS ASSOCIATE to have been, accessed, acquired, or disclosed during such breach. If BUSINESS ASSOCIATE does not possess the identity of all such individuals within 5 business days, BUSINESS ASSOCIATE shall notify COMPANY with such information as is available by that deadline and supplement immediately as additional information becomes available. Following notification by BUSINESS ASSOCIATE to COMPANY, COMPANY shall determine, in its sole discretion, whether BUSINESS ASSOCIATE or COMPANY shall provide notification to such individuals within the required 60 day deadline.

5. Corporate Compliance and Ethical Standards. BUSINESS ASSOCIATE agrees to adhere to and adopts the [Company] Compliance Program, including the [Company] Code of Compliance and Ethical Standards, a hard copy of which BUSINESS ASSOCIATE acknowledges receiving (the signed acknowledgement shall be attached hereto as Schedule A), and other Compliance Policies and Procedures that may be adopted by [Company] and made accessible to BUSINESS ASSOCIATE. BUSINESS ASSOCIATE further agrees to disseminate the above code to his/her applicable employees and other workforce members and require them to comply with same. The code has also been made available on the [Company] Intranet site (http://) and is publicly available on the [Company] Internet Web site (http://www.).

6. Ethics Complaints Hotline. BUSINESS ASSOCIATE acknowledges that he/she/it may address any issues or ask questions concerning ethical or legal conduct or report any potentially improper action, such as a suspected violation of the above privacy/security laws, [Company] policies and procedures, Federal health care program requirements, and/or criminal, civil or administrative law, by calling the [Company] Confidential Ethics Line (1.XXX.XXX.XXXX). BUSINESS ASSOCIATE may do so anonymously and without fear of retaliation or retribution of matters reported in good faith to raise legitimate concerns.

7. Termination of Contract. COMPANY may terminate this contract if COMPANY determines BUSINESS ASSOCIATE has violated any material term of this Agreement.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement, to be effective on _____.

BUSINESS ASSOCIATE		COMPANY
By:		By:
Title: Date:		Title: Date:

SCHEDULE A

[Company] Code of Compliance and Ethical Standards Acknowledgment
(Attached)

Attachment "A"

Checklist of ID Theft "Red Flags"

Patient Check-In and Registration (Specific protocols for these and related Red Flags are in Attachment "B")

1. **Any existing "Alert" indicated in the patient's record.**

2. **A patient who has an insurance number but who doesn't produce an insurance card or other physical documentation of insurance.**

A medical identity thief may succeed by obtaining the medical insurance number and other information about the victim. The absence of an actual insurance card suggests that the person being treated may not be the actual insured. (**Note**: This Red Flag has to be applied with caution because there are other reasons a patient may not have their insurance card).

3. **Patient lacks or refuses to provide identification.**

Caution should also be exercised here. Deferral of service should be discussed with the appropriate supervisor and notation made when a patient is asked to bring appropriate documentation to their next visit.

4. **The patient is recognized to be someone other than the individual being claimed.**

5. **The patient's Social Security Number appears invalid. The following are invalid:**

   - The first three digits are in the 800, 900, or 000 range;
   - The first three digits are in a range from 772 to 799;
   - The first three digits are 666;
   - The fourth and fifth digits are 00; or
   - The last four digits are 0000.

6. **Documents provided for identification appear to have been altered or forged.**

7. **The photograph or physical description on the identification is inconsistent with the appearance of the patient presenting the identification.**

8. **The patient fails to provide all required personal identifying information on a form or in response to notification that the form is incomplete.**

9. **Information on one form of identification is inconsistent with information on another form already in clinic or billing records; other discrepancies between check-in information versus prior account, insurance, or other existing information in the system. (Example: *signature doesn't match what's on file*).**

10. **Patient provides a post office box as a physical address**

11. **The patient is unable to authenticate their identity by correctly answering "challenge" questions based on information beyond what would be found in a wallet or credit report.**

Notice from patients, health plans, law enforcement, or others regarding possible identity theft in connection with a patient account

All staff who interact with patients (Customer Service, Billing, Compliance, Risk Management) should be alert to the following notices.

12. **The Clinic or Billing Department is notified that a patient has not been receiving statements or explanation of benefits (EOBs).**

13. **Mail sent to the patient is repeatedly returned as undeliverable although transactions continue to take place.**

14. **A complaint or question from a patient based on the patient's receipt of:**

    - a bill or claim for another individual
    - a bill or claim for a product or service that the patient denies receiving
    - a bill or claim from a healthcare provider that the patient never visited
    - an EOB or other notice for health services never received

15. **Complaint or question from a patient about the receipt of a collection notice from a bill collector.**

16. **Complaint or question from a patient about information added to a credit report by a healthcare provider or insurer.**

An entry in a credit report is a common way that a patient discovers that they have been a victim of medical identity theft.

17. **A dispute of a bill by a patient who claims to be the victim of *any type* of identity theft.**

A victim of *financial* identity theft may be more likely to also be a victim of *medical* identity theft. Victims of financial identity theft may have filed police reports about their case, which should be taken into account and raise an alert.

18. **A patient or insurance company report that coverage for legitimate medical services are being denied because insurance benefits have been depleted, or that a lifetime cap has been reached.**

Members of a family can be victimized by "looping", where a thief uses one family member's benefits and then turns to the next member when the first victim's benefits have run out.

19. **A notice or inquiry from an insurance investigator or a law enforcement agency.**

Employees have been known to exploit legitimate access to health files to use patients' identity and health information for financial and medical identity theft.

Treatment, Payment, and Healthcare Operations

20. **Records indicating medical treatment that is inconsistent with the physical examination or medical history as reported by the patient.**

Medical records that show substantial discrepancies in age, race, and other physical descriptions (e.g., blood type) may be evidence of medical identity theft. Those who review medical records (clinic staff, billing operations, EMR department, compliance coders, etc.) should be alert to discrepancies.

21. **Patient protected health information (PHI) found trash receptacles or on other open areas in the clinic/office.**

The Facility should review and assess if there is risk of identity theft to any patient whose PHI was found to be unsecure.

Monitoring Activities (Data Analytics)

Audit logs of employee/staff access to billing and EMR systems, with custom rules and thresholds to alert the Privacy and Security team to highly suspicious activities, will be routinely reviewed. Audit trails can be reviewed manually or through automated processes. Certain claims transaction analyses to monitor for fraud and abuse may apply. The following are continuous monitoring activities to be conducted:

22. **The Social Security Number (SSN) provided is the same as assigned to other patients.**

Routine data matches of SSN and patient names to be performed by IT Security and Billing.

23. **The SSN furnished by the patient has not yet been issued or is otherwise invalid.**

Examples: (i) The SSN is listed on the Social Security Administration's public Death Master File; (ii) there is a lack of correlation between the defined SSN ranges and date of birth.

24. **The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other patients.**

25. **Last names of staff members matching patient names.**

Performing user/patient last name matches can identify potential inappropriate snooping by family (HIPAA privacy violation).

26. **Unusual volumes of patient record access and printing.**

27. **Inappropriate services for the patients' demographic (e.g., women's services for men, pediatric services for adults)**

28. **Prescriptions in unusually high frequencies.**

[TEMPLATE]

Prevention of Medical Identity Theft Policy – Letter Regarding Security Breach Incident

[Date]

BY CERTIFIED MAIL, RETURN RECEIPT REQUESTED

[Patient Name][Patient Address][Patient Address]

Re: Preventing Identity Theft

Dear _____:

We are writing to you because of a recent security incident at [Name of Organization].

[Describe what happened in general terms, what kind of personal information was involved, and what you are doing in response.]

To protect yourself from the possibility of identity theft, we recommend that you have a fraud alert placed on their credit files. You can add this alert by contacting one of the three credit reporting agencies. When you request a fraud alert from one bureau, it will notify the other two for you.

Your credit file will be flagged with a statement that says you may be a victim of fraud and that creditors should contact you before opening new accounts. You will receive letters from all three credit agencies with instructions on how to get a free copy of your credit report from each agency.

Equifax
P.O Box 740241
Atlanta GA 30374-0241
www.equifax.com
1-800-525-6285

Experian
P.O. Box 9534
Allen, TX 75013
www.experian.com
1-888-EXPERIAN
1-888-397-3742

Trans Union
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton CA 92834-6790
www.transunion.com
1-800-680-7289

When you receive your credit reports review them carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and social security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police office and file a police report of identity theft. Get a copy of the police report as you may need to give copies of the report to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit report every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place. Under federal law, you are entitled to receive one free comprehensive disclosure/report of all the information in your credit file from each of the three national credit bureaus listed above once every 12 months.

We apologize for this incident and sincerely regret any inconvenience that these events and responding to this notice may cause you." For more information on identity theft, we suggest that you visit the Web site of the www.privacyrights.com (or the Federal Trade Commission at www.consumer/gov/idtheft.)

If there is anything we can do to assist you, please call our Compliance and Risk Department at 972.743.3803.

MedicalEdge
HEALTHCARE GROUP, INC

IDENTITY THEFT PREVENTION AND ACTION

DEPARTMENTS: Compliance and Information Technology	POLICY DESCRIPTION: Implementation of an Identity Theft Prevention Program
Date of Issue: 05.01.2009	Date of Last Revision: **N/A**
Effective Date: **05.01.2009**	Compliance Policy Manual:

SCOPE

This policy applies to MedicalEdge Healthcare Group, Inc. (MEHG or the Company) and all providers, facilities, and clinics (collectively "Facilities") of its physician group clients, as well as external billing individuals or entities utilized by the physician groups or MEHG.

PURPOSE:

To establish and maintain an Identity Theft Prevention Program (the "Program") to detect, prevent and mitigate the occurrence of identity theft for patients who receive services from physician group Facilities. Identity theft and specifically "medical" identity theft can lead to inappropriate medical care, as well as financial harm. This Program is intended to follow all federal and state laws, and reporting requirements regarding incidents of identity theft, including the Red Flags Rule under the Federal Fair and Accurate Credit Transactions Act.

POLICY:

MEHG and physician group Facilities are expected to respond and report any "Red Flags" that indicate the possibility of identity theft involving a patient. The Company and Facilities should take steps to implement controls to detect, prevent, and mitigate the misuse of a patient's identity to commit identity theft. Potential Red Flags and this Policy and related processes will be updated on a regular basis.

- The Company and Facilities can identify relevant patterns, practices, and specific forms of activity that are "Red Flags" signaling possible identity theft, and to incorporate those Red Flags into procedures and protocols to detect and prevent future occurrences.
- Providers, staff, and employees should be alert for the possibility of patient identity theft and be aware of the Red Flags that affect their area of responsibility. See **Attachment "A"** for a checklist of currently recognized Red Flags and processes to be utilized for detection.
- Providers, staff, and employees are expected to respond to recognized Red Flags and immediately report potential identity theft incidents to their supervisor and/or MEHG's IT Information Security Officer and Chief Compliance Officer.
- The MEHG Compliance Department with support from the IT Information Security Officer is responsible for implementing and maintaining a written Identity Theft Prevention Program.

Applicable Definitions:

- **Identity theft** – A fraud committed or attempted using the identifying information of another person without authority.
- ***Medical* identity theft** – A common type of identity theft that refers to the misuse of another individual's personally identifiable information to obtain or bill for medical services or goods.
- **Red Flag** – A pattern, practice, or specific activity that could indicate identity theft.

PROCEDURE:

All providers, staff, and employees should prevent any unauthorized access, use, or disclosure of patients' identifying information in accordance with MEHG conduct, privacy and security policies. Appropriate steps are to be taken if an identity theft Red Flag or suspicious activity is recognized.

- **Detecting Red Flags** – Providers and staff should be alert to discrepancies in documents and patient information that suggest the risk of identity theft or fraud. Facilities should verify and authenticate patient identity, residence, and insurance coverage at the time of registration and check-in. A specific protocol for patient registration and check-in is provided in **Attachment "B"**.
- **Responding to Red Flags** – If identity theft and fraudulent activity is suspected, or if a patient claims to be a victim of identity theft, the Compliance Department and Information Security Officer will respond and investigate the situation.
  - Staff and employees should gather all documentation and report the Red Flag or situation to his or her supervisor, or directly to the Information Security Officer or Chief Compliance Officer. Third party experts can be consulted to assist in investigating, if warranted.
  - MEHG security and compliance officials will assess the situation and determine if identity theft has occurred, and notify law enforcement if needed.
- **Informing the Patient about Identity Theft** – MEHG and the Facilities should inform the patient, in writing, of possible unauthorized use of their personal identifying information. Efforts should also be made to directly contact the patient by telephone or in-person so they can take appropriate steps to protect their identity. Notice should only be delayed if law enforcement informs that disclosure of the identity theft or breach would impede a criminal investigation. The required notice should be provided without unreasonable delay after the law enforcement agency communicates its determination that notice will no longer impede the investigation.
  - A formal letter should be mailed to the patient via certified postal mail, return receipt requested. The letter should state the reason the clinic feels the patient is a victim of identity theft and the recommended steps the patient should undertake.
  - The patient should be given information on how to alert credit bureaus to the potential identity theft.
- **Mitigating Identity Theft Incidents** – If following investigation, it appears that the patient has been a victim of identity theft; the following actions are recommended:
  - MEHG and the affected facility or clinic should notify the appropriate law enforcement agency and cancel active transactions. A Red Flag "Alert" should be placed into the patient's account and medical record.
  - The impacted facility or clinic should cease collection on open accounts that resulted from identity theft. If accounts had been referred to collection agencies, the collection agencies will be instructed to cease collection activity.
  - The patient should be encouraged to file a police report if not already done.
  - The facility or clinic is expected to cooperate with any law enforcement investigation relating to the identity theft incident.
  - If an adverse report had been made to a consumer reporting agency, MEHG or the affected Facility should notify the agency that the account was not the responsibility of the patient.
  - If appropriate, MEHG should consider offering the patient the option of enrolling in a credit monitoring service for a defined period of time.
  - Further remedial actions and notifications should be considered based on the circumstances.

- **Patient File Extraction** – For victims of identity theft, the Facility physician should review the patient's medical record to determine whether documentation was made that resulted in inaccurate information in the record. If inaccuracies due to identity theft exist, a notation can be made in the record.
  - Best efforts should be made to remove fraudulent information from the victim's medical file to be maintained separately.
  - The facility staff should assess whether any other records or ancillary service providers are linked to inaccurate information. Any additional records containing information relevant to the identity theft will be identified and appropriate action taken.
- **HIPAA security standards** – If the fraudulent activity involves protected health information (PHI) as defined by the Health Insurance Portability and Accountability Act (HIPAA), MEHG and the Facilities should apply HIPAA security policies and procedures to the response.

REFERENCES:

Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rules, 72 Fed. Reg. 63718 (Nov. 9, 2007); 16 C.F.R. § 681.2, implementing 15 U.S.C. § 1681m(e).

Sample Business Associate Agreement

This Business Associate Agreement (the "Agreement") is made and entered into effective as of _____[DATE], by and between [NAME OF COVERED ENTITY]

(“Covered Entity”), and _____, a _____ [enter corporate entity type and state of formation]("Business Associate"). In consideration of the mutual promises below, and other good and valuable consideration, the sufficiency of which is hereby acknowledged, the parties agree as follows:

1. DEFINITIONS

Terms used in this Agreement that are specifically defined in HIPAA shall have the same meaning as set forth in HIPAA. A change to HIPAA which modifies any defined HIPAA term, or which alters the regulatory citation for the definition shall be deemed incorporated into this Agreement.

1.1 **“Business Associate”** shall mean the entity described above. Where the term "business associate" appears without an initial capital letter, it shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 CFR § 160.103.

1.2 **“Covered Entity”** shall mean [NAME OF COVERED ENTITY ABOVE].

1.3 **“Data Aggregation”** shall have the meaning given to the term under the Privacy Rule, including, but not limited to, 45 CFR § 164.501.

1.4 **“Designated Record Set”** shall have the meaning given to the term under the Privacy Rule, including, but not limited to, 45 CFR §164.501.

1.5 **“Electronic Protected Health Information”** and/or **“EPHI”** shall have the same meaning as the term “electronic protected health information" in 45 CFR § 160.103, and shall include, without limitation, any EPHI provided by Covered Entity or created or received by Business Associate on behalf of Covered Entity.

1.6 **“HIPAA”** means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-91, as amended, and related HIPAA regulations (45 CFR. Parts 160-164).

1.7 **“HITECH”** means the Health Information Technology for Economic and Clinical Health Act, found in Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-005.

1.8 **“Individual”** shall have the meaning given to the term under the Privacy Rule, including, but not limited to, 45 CFR § 160.103. It shall also include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

1.9 **“Privacy Rule”** shall mean the Standards for Privacy of Individually Identifiable Health Information, and Security Standards for the Protection of Electronic Protected Health Information (the “Security Rule”), that are codified at 45 CFR parts 160 and 164, Subparts A, C, and E and any other applicable provision of HIPAA, and any amendments thereto, including HITECH.

1.10 **“Protected Health Information”** and/or **“PHI”** shall have the meaning given to the term under the Privacy Rule, including but not limited to, 45 CFR §

164.103, and shall include, without limitation, any PHI provided by Covered Entity or created or received by Business Associate on behalf of Covered Entity. Unless otherwise stated in this Agreement, any provision, restriction, or obligation in this Agreement related to the use of PHI shall apply equally to EPHI.
1.11 **"Required By Law"** shall have the meaning given to the term under the Privacy Rule, including but not limited to, 45 CFR § 164.103, and any additional requirements created under HITECH.
1.12 **"Secretary"** shall mean the Secretary of the Department of Health and Human Services or his designee.
1.13 **"Security Incident"** shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system as provided in 45 CFR § 164.304.
1.14 **"Services Agreement"** shall mean the underlying agreement(s) that outline the terms of the services that Business Associate agrees to provide to Covered Entity and that fall within the functions, activities or services described in the definition of "Business Associate" at 45 CFR § 160.103.
1.15 **"Unsecured PHI"** shall have the same definition that the Secretary gives the term in guidance issued pursuant to § 13402 of HITECH.

2. BUSINESS ASSOCIATE OBLIGATIONS
2.1 Business Associate agrees that it shall only use and disclose PHI in accordance with the terms of this Agreement or as is Required By Law.
2.2 Business Associate shall not use or disclose PHI except for the purpose of performing Business Associate's obligations to Covered Entity, as such use or disclosure is limited by this Agreement. These obligations are as follows: [INSERT PERMITTED USES AND DISCLOSURES OR REFER TO AN ATTACHED DOCUMENT THAT DESCRIBES THE SERVICES TO BE PROVIDED TO COVERED ENTITY.]
2.3 Business Associate shall not use or disclose PHI in any manner that would constitute a violation of the Privacy Rule. So long as such use or disclosure does not violate the Privacy Rule or this Agreement, Business Associate may use PHI: (a) as is necessary for the proper management and administration of Business Associate's organization, or (b) to carry out the legal responsibilities of Business Associate, as provided in 45 CFR § 164.504(e)(4).
2.4 Business Associate will ensure that any agents, including subcontractors, to whom it provides PHI agree in writing to the same restrictions and conditions, including but not limited to those relating to termination of the contract for improper disclosure, that apply to Business Associate with respect to such information. Further, Business Associate shall implement and maintain sanctions against agents and subcontractors, if any, that violate such restrictions and conditions. Business Associate shall terminate any agreement with an agent or subcontractor, if any, who fails to abide by such restrictions and obligations. Business Associate shall not provide any PHI to any third party or subcontract any Services without Covered Entity's express written permission.
2.5 Business Associate shall develop, implement, maintain, and use appropriate safeguards to prevent any use or disclosure of the PHI or EPHI other than as provided by this Agreement, and to implement administrative, physical, and

technical safeguards as required by sections 164.308, 164.310, 164.312 and 164.316 of title 45, Code of Federal Regulations and HITECH in order to protect the confidentiality, integrity, and availability of EPHI or PHI that Business Associate creates, receives, maintains, or transmits, to the same extent as if Business Associate were a Covered Entity. See HITECH § 13401.
2.6 The additional requirements of Title XIII of HITECH that relate to privacy and security and that are made applicable with respect to covered entities shall also be applicable to Business Associate and shall be and by this reference hereby incorporated into this Agreement.
2.7 Business Associate agrees to adopt the technology and methodology standards provided in any guidance issued by the Secretary pursuant to HITECH §§ 13401-13402.
2.8 Business Associate agrees to mitigate any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement and to notify covered entity of any breach of unsecured PHI, as required under HITECH § 13402.
2.9 Business Associate shall report, in writing, to Covered Entity any use or disclosure of PHI that is not authorized by the Agreement. Such written notice shall be provided to Covered Entity within five (5) business days of becoming aware of such use or disclosure.
2.10 In the case of a breach of Unsecured PHI, Business Associate shall, following the discovery of a breach of such information, notify the Covered Entity of such breach. The notice shall include the identification of each individual whose Unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or disclosed during the breach. If the breach involves the Unsecured PHI of more than 500 residents of [State] or residents of a certain region, or is reasonably believed to have been accessed, acquired or disclosed during such incident, [Entity] will also notify the prominent media outlets. The media outlets must serve the geographic area affected.
2.11 Business Associate must obtain, prior to making any permitted disclosure as set forth in Section 2.2, reasonable assurances from such third party that such PHI will be held secure and confidential as provided pursuant to this Agreement and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and that any breaches of confidentiality of the PHI which becomes known to such third party will be immediately reported to Business Associate. As part of obtaining this reasonable assurance, Business Associate agrees to enter into a Business Associate Agreement with each of its subcontractors pursuant to 45 CFR § 164.308(b)(1) and HITECH § 13401.
2.12 Business Associate shall make PHI in Designated Record Sets that are maintained by Business Associate or its agents or subcontractors, if any, available to Covered Entity for inspection and copying within ten (10) days of a request by Covered Entity to enable Covered Entity to fulfill its obligations under the Privacy rule, including, but not limited to, 45 CFR § 164.524.
2.13 Within ten (10) days of receipt of a request from Covered Entity for an amendment of PHI or a record about an Individual contained in a Designated Record Set, Business Associate or its agents or subcontractors, if any, shall make such PHI available to Covered Entity for amendment and shall incorporate any such amendment to enable Covered Entity to fulfill its obligations under the

Privacy Rule, including, but not limited to, 45 CFR § 164.524. If an Individual requests an amendment of PHI directly from Business Associate or its agents or subcontractors, if any, Business Associate must notify Covered Entity in writing within five (5) days of the request. Any denial of amendment of PHI maintained by Business Associate or its agents or subcontractors, if any, shall be the responsibility of Covered Entity. Upon the approval of Covered Entity, Business Associate shall appropriately amend the PHI maintained by it, or any agents or subcontractors.

2.14 Within ten (10) days of notice by Covered Entity of a request for an accounting of disclosures of PHI, Business Associate and any agents or subcontractors shall make available to Covered Entity the information required to provide an accounting of disclosures to enable Covered Entity to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR § 164.528. Except in the case of a direct request from an Individual for an accounting related to treatment payment or operations disclosures through an electronic health record, if the request for an accounting is delivered directly to Business Associate or its agents or subcontractors, if any, Business Associate shall within five business (5) days of a request notify Covered Entity about such request. Covered Entity shall either inform Business Associate to provide such information directly to the Individual, or it shall request the information to be immediately forwarded to Covered Entity for compilation and distribution to such Individual. In the case of a direct request for an accounting from an Individual related to treatment, payment or operations disclosures through electronic health records, Business Associate shall provide such accounting to the Individual in accordance with HITECH § 13405(c). Business Associate shall not disclose any PHI unless such disclosure is Required by Law or is in accordance with this Agreement. Business Associate shall document such disclosures. Notwithstanding Section 4.4, Business Associate and any agents or subcontractors shall continue to maintain the information required for purposes of complying with this Section 2.12 for a period of six (6) years after termination of the Agreement.

2.15 Business Associate shall make its internal practices, books and records relating to the use and disclosure of PHI available to the Secretary for purposes of determining Covered Entity's compliance with the Privacy Rule. Business Associate shall notify Covered Entity regarding any PHI that Business Associate provides to the Secretary concurrently with providing such PHI to the Secretary, and upon request by Covered Entity, shall provide Covered Entity with a duplicate copy of such PHI.

2.16 Business Associate and its agents or subcontractors, if any, shall only request, use and disclose the minimum amount of PHI necessary to accomplish the purpose of the request, use or disclosure. Business Associate agrees to comply with the Secretary's guidance on what constitutes minimum necessary. *See* HITECH § 13405.

2.17 Business Associate acknowledges that Business Associate has no ownership rights related to the PHI.

2.18 Business Associate and its subcontractors or agents, if any, shall retain any PHI throughout the term of the Agreement.

2.19 Unless greater coverage is required under any other agreement between Covered Entity and Business Associate for the provision of services related to this Agreement, Business Associate shall maintain or cause to be maintained the following insurance covering itself and each subcontractor or agent, if any, through whom Business Associate provides services; (i) a policy of commercial general liability and property damage insurance, and electronic data processing insurance, with limits of liability not less than two million dollars ($2,000,000) per occurrence and two million dollars ($2,000,000) annual aggregate and (ii) such other insurance or self insurance as shall be necessary to insure it against any claim or claims for damages arising under this Agreement or from violating Business Associate's own obligations under HIPAA and HITECH (*see* HITECH § 13404), including but not limited to, claims or the imposition of administrative penalties and fines on Business Associate or its subcontractors or agents, if any, arising from the loss, theft, or unauthorized use or disclosure of PHI. Such insurance coverage shall apply to all site(s) of Business Associate and to all services provided by Business Associate or any subcontractors or agents under this Agreement.
2.20 During the term of this Agreement, Business Associate shall notify Covered Entity within twenty-four (24) hours of any suspected or actual Security Incident or breach of security, intrusion or unauthorized use or disclosure of PHI or EPHI and/or any actual or suspected use or disclosure of data in violation of any applicable federal or state laws or regulations, or any legal action against Business Associate arising from an alleged HIPAA violation. Business Associate shall take (i) prompt action to correct any such deficiencies and (ii) any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations.
2.21 Within ten (10) business days of a written request by Covered Entity, Business Associate and its agents or subcontractors, if any, shall allow Covered Entity to conduct a reasonable inspection of the facilities, systems, books, records, agreements, policies and procedures relating to the use or disclosure of PHI pursuant to this Agreement for the purpose of determining whether Business Associate has complied with this Agreement and HITECH; provided, however, that (i) Business Associate and Covered Entity mutually agree in advance upon the scope, location and timing of such an inspection; and (ii) Covered Entity shall protect the confidentiality of all confidential and proprietary information of Business Associate to which Covered Entity has access during the course of such inspection.
2.22 Except as otherwise limited in this Agreement, Business Associate may use PHI to provide Data Aggregation services to Covered Entity as permitted by 45 CFR §164.504(e)(2)(I)(B).
2.23 If Business Associate knows of a pattern of activity or practice by the Covered Entity that constitutes a material breach or violation of the Covered Entity's obligations under this Agreement, Business Associate will take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful within a period of 30 days, Business Associate will either: 1) terminate the Agreement, if feasible; or 2) report the problem to the Secretary.

3. COVERED ENTITY OBLIGATIONS

3.1 Covered Entity shall provide Business Associate with the notice of any privacy practices that Covered Entity produces in accordance with 45 CFR § 164.520, as well as any changes to such notice.
3.2 Covered Entity shall provide Business Associate with notice of any changes to, revocation of, or permission by Individual to use or disclose PHI, if such changes affect Business Associate's permitted uses or disclosures, within a reasonable period of time after Covered Entity becomes aware of such changes to or revocation of permission.
3.3 Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to or must comply with in accordance with 45 CFR § 164.522 and HITECH § 13405(a).
3.4 Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

4. TERMINATION

4.1 The term of this Agreement shall be effective as of the date of this Agreement and continue until terminated by Covered Entity or any underlying Services Agreement expires or is terminated. Any provision related to the use, disclosure, access, or protection of EPHI or PHI or that by its terms should survive termination of this Agreement shall survive termination.
4.2 A breach by Business Associate, or its agents or subcontractors, if any, of any provision of this Agreement, as determined by Covered Entity, shall constitute a material breach of the Agreement. If Business Associate breaches this Agreement, Covered Entity may, in its discretion: (i) immediately terminate this Agreement; (ii) provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement if Business Associate does not promptly cure the breach or end the violation within a period not to exceed 30 days; or (iii) report the violation to the Secretary if neither termination nor cure is feasible.
4.3 Covered Entity may terminate this Agreement effective immediately, if (i) Business Associate is named as a defendant in a criminal proceeding for a violation of HIPAA, HITECH, or other security or privacy laws or (ii) there is a finding or stipulation that Business Associate has violated any standard or requirement of HIPAA, HITECH, or other security or privacy laws in any administrative or civil proceeding in which Business Associate is involved.
4.4 Upon termination of this Agreement for any reason, Business Associate shall return, or at Covered Entity’s request, destroy all PHI that Business Associate or its agents or subcontractors, if any, still maintain in any form, and shall retain no copies of such PHI. If return or destruction is not feasible, Business Associate shall explain to Covered Entity why conditions make the return or destruction of such PHI not feasible. If Covered Entity agrees that the return or destruction of PHI is not feasible, Business Associate shall retain the PHI, subject to all of the protections of this Agreement, and shall make no further use of such PHI. If Business Associate elects to destroy the PHI, Business Associate shall certify in writing to Covered Entity that such PHI has been destroyed.
4.5 If this Agreement is terminated for any reason, Covered Entity may also terminate the Services Agreement between the parties. This provision shall

supersede any termination provision to the contrary which may be set forth in the Services Agreement.

5. MISCELLANEOUS

5.1 A reference in this Agreement to a section in the Privacy Rule means the Privacy Rule section as in effect or as amended.

5.2 Business Associate and any of its subcontractors and agents shall indemnify, hold harmless and defend Covered Entity and its employees, officers, directors, agents, and contractors from and against any and all claims, losses, liabilities, costs, attorneys' fees, and other expenses incurred as a result of or arising directly or indirectly out of or in connection with Business Associate's or its subcontractors' or agents' breach of this Agreement, violation of HIPAA, HITECH or other applicable law, or otherwise related to the acts or omissions of Business Associate or its subcontractors or agents.

5.3 Business Associate may not subcontract any Services or assign any rights, nor may it delegate its duties, under this Agreement without the express written consent of Covered Entity.

5.4 Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate, or their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

5.5 The parties are independent contractors and nothing in this Agreement shall be deemed to make them partners or joint venturers.

5.6 If any modification to this Agreement is Required By Law or required by HITECH or any other federal or state law affecting this Agreement, or if Covered Entity reasonably concludes that an amendment to this Agreement is needed because of a change in federal or state law or changing industry standards, Covered Entity shall notify Business Associate of such proposed modification(s) ("Legally-Required Modifications"). Such Legally Required Modifications shall be deemed accepted by Business Associate and this Agreement so amended, if Business Associate does not, within thirty (30) calendar days following the date of the notice (or within such other time period as may be mandated by applicable state or federal law), deliver to Covered Entity its written rejection of such Legally-Required Modifications.

5.7 Business Associate will comply with all appropriate federal and state security and privacy laws, to the extent that such laws apply to Business Associate or are more protective of Individual privacy than are the HIPAA laws.

5.8 All notices which are required or permitted to be given pursuant to this Agreement shall be in writing and shall be sufficient in all respects if delivered personally, by electronic facsimile (with a confirmation by registered or certified mail placed in the mail no later than the following day), or by registered or certified mail, postage prepaid, addressed to a party as indicated below:

If to Business Associate:	If to Covered Entity:
INSERT ADDRESS	INSERT ADDRESS

Notice shall be deemed to have been given upon transmittal thereof as to communications which are personally delivered or transmitted by electronic

facsimile and, as to communications made by United States mail, on the third (3rd) day after mailing. The above addresses may be changed by giving notice of such change in the manner provided above for giving notice.

5.9 If any provision of this Agreement is determined by a court of competent jurisdiction to be invalid, void, or unenforceable, the remaining provisions hereof shall continue in full force and effect.

5.10 This Agreement contains the entire understanding between the parties hereto and shall supersede any other oral or written agreements, discussions and understandings of every kind and nature, including any provision in any Services Agreement. No modification, addition to or waiver of any right, obligation or default shall be effective unless in writing and signed by the party against whom the same is sought to be enforced. No delay or failure of either party to exercise any right or remedy available hereunder, at law or in equity, shall act as a waiver of such right or remedy, and any waiver shall not waive any subsequent right, obligation, or default.

5.11 This Agreement shall be governed by state law without respect to its conflict of law principles.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their respective duly authorized representatives as of the dates set forth below.

BUSINESS ASSOCIATE	**COVERED ENTITY**
By:	By:
Name:	Name:
Title:	Title:

Attachment "B"

Protocol: Verifying Patient Identity at Time of Registration/Check-in

It is the practice of the clinic/facility ("Facility") to verify patient identity at time of registration. The Facility will, to the extent feasible, request documentation of the patient's *identity*, *residential address*, and *insurance coverage* at time of registration as part of the Identity Theft Prevention Program.

Patient Check-In and Registration

The following **Notice** is recommended to be available at the Facility's front desk:

NEW FEDERAL LAWS require us to carefully and thoroughly verify your identity

As you may be aware, identity theft is the fastest growing crime in the U.S. *Medical* identity theft is someone using your information to fraudulently receive healthcare, and it is the fastest growing type of identity theft.

In an ongoing effort to safeguard your identity, we carefully review documents that you present and in some cases may ask you for more information. This is intended to protect you. Please be prepared to provide the information that we request, including:

1. Driver's License or other Photo Identification
2. Your health insurance card
3. Your Social Security card or number
4. Residence information
5. Date of Birth or other personal identifying information

From time to time we may need to ask you for additional information. We are sorry for the inconvenience this may cause. Please remember, we want to protect you and it is the law.

Sincerely,

[Facility Name]

Procedures:

1. When a patient calls to request or confirm an appointment, the patient will be asked to bring the following documentation at check-in for the appointment –
    - Driver's license or other government-issued photo identification (ID)
    - Current insurance card
    - Alert the patient that if their photo ID does not show their current residential address (or if a P.O. Box is listed), then the patient should also bring a recent utility bill or other correspondence showing current residence.

- If the patient is a minor, the patient's parent or guardian should bring the information listed.

2. When the patient arrives for the appointment, they will be asked to produce the documents listed above. NOTE: This requirement may be limited for patients who have been seen within the last six months (e.g., insurance information only) or for patients well-known to the Facility—judgment and discretion should be exercised.

3. Note: It is NOT recommended that copies be made of patient ID information (Driver's License, Social Security card, etc.) to be maintained as this information can increase the risk of identity theft.

4. If the patient is unable to produce the requested documents, it is appropriate to consider alternative options to verify the patient's identity. Challenge questions can be considered based on information in the patient's account [e.g., last 4 digit of their Social Security Number (SSN)].

5. If the patient has not completed the registration form within the last six months, a new registration form should be completed upon registration or check in.

6. In the following circumstances, staff should be alert for the possibility of identity theft:

   <u>Registration</u>

   a. Any existing Red Flag "Alert" indicated in the patient's file or medical record.
   b. A patient who has an insurance number but who doesn't produce an insurance card or other physical documentation of insurance.
   c. Patient lacks or refuses to provide identification.
   d. The patient is recognized to be someone other than the individual being claimed.
   e. The patient's SSN appears invalid. The following are invalid –
      - The first three digits are in the 800, 900, or 000 range
      - The first three digits are in a range from 772 to 799
      - The first three digits are 666
      - The fourth and fifth digits are 00
      - The last four digits are 0000
   f. The SSN or other identifying information furnished by the patient is the same as identifying information provided by other patients.
   g. Documents provided for identification appear to have been altered or forged.
   h. The photograph or physical description on the identification is inconsistent with the appearance of the patient presenting the identification.
   i. The patient fails to provide all required personal identifying information on a form or in response to notification that the form is incomplete
   j. Information on one form of identification is inconsistent with information on another form already in clinic; other discrepancies between check-in information versus prior account, insurance, or other existing information in the system.
   k. The patient's signature does not match a signature on file in the organization's records.
   l. Patient provides a post office box as a physical address.

m. The patient is unable to authenticate their identity by correctly answering "challenge" questions based on information beyond what would be found in a wallet or credit report.

Notice provided by patient

n. The patient informing that they have not been receiving statements or explanation of benefits (EOBs).
o. Complaint or question from a patient about the receipt of a collection notice from a bill collector
p. A complaint or question from a patient based on the patient's receipt of (i) a bill for another individual; (ii) a bill for a product or service that the patient denies receiving; (iii) a bill or claim from a healthcare provider that the patient never visited; (iv) an EOB or other notice for health services never received.

Miscellaneous

q. Any information indicating that the patient's medical treatment is inconsistent with the physical examination or medical history as reported by the patient.

7. If the patient does not have all the identifying information requested (and additional authentication is unsuccessful) it is appropriate to inform the patient that he or she cannot be seen until more documentation is provided.

8. If a Red Flag or other improper activity is detected, caution is urged before any action is taken. If a patient lacks or refuses to provide identification deferral of service should be discussed with the appropriate supervisor, and notation made indicating the patient has been asked to bring appropriate documentation to the next visit. There also may be reasons a patient may not have their insurance card but has other identifying information and coverage can be verified.

9. If a Red Flag is observed, staff should gather all documentation and report the matter to a supervisor at the Facility, or to the designated Information Security Officer or Chief Compliance Officer. The Compliance Department will assist in determining whether identity theft has occurred and what action steps need to be taken.

10. Prescription Medications and Protecting of Patient Health Information: The Facility should continue to be alert and sensitive to the safeguarding of patient health information and follow protocols required under the privacy and security requirements of the Health Insurance Portability and Accountability Act (HIPAA).

r. Staff should review patient instructions as to whom health information can be released (Privacy Directive).
s. If someone other than the patient will be picking-up prescription medication for the patient, staff should verify the individual's identity and require signing a receipt to confirm receipt of the medication.