NOTICE OF PRIVACY PRACTICES

This copy is provided for you to review while in our office. If you would like a copy for yourself you may download a copy from our website: www.smilestartersdental.com or we will provide a written copy for you at your request.

Dr. Rafael Rivera Jr., DDS, PLLC dba Smile Starters / Wilmington Dental Care

Rafael Rivera Jr DDS PLLC dba

Smile Starters / Wilmington Dental Care

NOTICE OF PRIVACY PRACTICES

(includes Omnibus changes as of March 2013)

Effective Date: 2/3/2016

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

PLEASE REVIEW IT CAREFULLY.

If you have any questions about this Notice of Privacy Practices ('Notice'), please contact:

Privacy Officer: Tamara Rivera

Phone Number: (704) 816-1404

Section A: Who Will Follow This Notice?

This Notice describes Rafael Rivera Jr DDS PLLC (hereafter referred to as 'Provider') Privacy Practices and that of any workforce member authorized to create medical information referred to as Protected Health Information (PHI) which may be used for purposes such as Treatment, Payment and Healthcare Operations. These workforce members may include:

- all departments and units of the Provider.
- any member of a volunteer group.
- all employees, staff and other Provider personnel.
- any entity providing services under the Provider's direction and control will follow the

terms of this notice. In addition, these entities, sites and locations may share medical information with each other for Treatment, Payment or Healthcare Operational purposes described in this Notice.

Section B: Our Pledge Regarding Medical Information

We understand that medical information about you and your health is personal. We are committed to protecting medical information about you. We create a record of the care and services you receive at the Provider. We need this record to provide you with quality care and to comply with certain legal requirements. This Notice applies to all of the records of your care generated or maintained by the Provider, whether made by Provider personnel or your personal doctor.

This Notice will tell you about the ways in which we may use and disclose medical information about you. We also describe your rights and certain obligations we have regarding the use and disclosure of medical information.

We are required by law to:

- Make sure that medical information that identifies you is kept private;
- Give you this Notice of our legal duties and privacy practices with respect to medical information about you; and
- Follow the terms of the Notice that is currently in effect.

Section C: How We May Use and Disclose Medical Information about You

The following categories describe different ways that we use and disclose medical information. For each category of uses or disclosures we will explain what we mean and try to give some examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories.

- **Treatment.** We may use medical information about you to provide you with medical treatment or services. We may disclose medical information about you to doctors, nurses, technicians, health care students, or other Provider personnel who are involved in taking care of you at the Provider. For example, a doctor treating you for a broken leg may need to know if you have diabetes because diabetes may slow the healing process. In addition, the doctor may need to tell the dietitian if you have diabetes so that we can arrange for appropriate meals. Different departments of the Provider also may share medical information about you in order to coordinate different items, such as prescriptions, lab work and x-rays. We also may disclose medical information about you to people outside the Provider who may be involved in your medical care after you leave the Provider.

- **Payment.** We may use and disclose medical information about you so that the treatment and services you receive at the Provider may be billed and payment may be collected from you, an insurance company or a third party. For example, we may

need to give your health plan information about surgery you received at the Provider so your health plan will pay us or reimburse you for the procedure. We may also tell your health plan about a prescribed treatment to obtain prior approval or to determine whether your plan will cover the treatment.

- **Healthcare Operations.** We may use and disclose medical information about you for Provider operations. These uses and disclosures are necessary to run the Provider and make sure that all of our patients receive quality care. For example, we may use medical information to review our treatment and services and to evaluate the performance of our staff in caring for you. We may also combine medical information about many Provider patients to decide what additional services the Provider should offer, what services are not needed, and whether certain new treatments are effective. We may also disclose information to doctors, nurses, technicians, health care students, and other Provider personnel for review and learning purposes. We may also combine the medical information we have with medical information from other Providers to compare how we are doing and see where we can make improvements in the care and services we offer. We may remove information that identifies you from this set of medical information so others may use it to study health care and health care delivery without learning a patient's identity.

- **Appointment Reminders.** We may use and disclose medical information to contact you as a reminder that you have an appointment for treatment or medical care at the Provider.

- **Treatment Alternatives.** We may use and disclose medical information to tell you about or recommend possible treatment options or alternatives that may be of interest to you.

- **Health-Related Benefits and Services.** We may use and disclose medical information to tell you about health-related benefits or services that may be of interest to you.

- **Fundraising Activities.** We may use information about you to contact you in an effort to raise money for the Provider and its operations. We may disclose information to a foundation related to the Provider so that the foundation may contact you about raising money for the Provider. We only would release contact information, such as your name, address and phone number and the dates you received treatment or services at the Provider. If you do not want the Provider to contact you for fundraising efforts, you must notify us in writing and you will be given the opportunity to 'Opt-out' of these communications.

• Authorizations Required

We will not use your protected health information for any purposes not specifically allowed by Federal or State laws or regulations without your written authorization; this includes uses of your PHI for marketing or sales activities.

- **Emergencies.** We may use or disclose your medical information if you need emergency treatment or if we are required by law to treat you but are unable to obtain your consent. If this happens, we will try to obtain your consent as soon as we reasonably can after we treat you.

- ## Psychotherapy Notes

Psychotherapy notes are accorded strict protections under several laws and regulations. Therefore, we will disclosure psychotherapy notes only upon your written authorization with limited exceptions.

- **Communication Barriers.** We may use and disclose your health information if we are unable to obtain your consent because of substantial communication barriers, and we believe you would want us to treat you if we could communicate with you.

- **Provider Directory.** We may include certain limited information about you in the Provider directory while you are a patient at the Provider. This information may include your name, location in the Provider, your general condition (e.g., fair, stable, etc.) and your religious affiliation. The directory information, except for your religious affiliation, may also be released to people who ask for you by name. Your religious affiliation may be given to a member of the clergy, such as a priest or rabbi, even if they do not ask for you by name. This is so your family, friends and clergy can visit you in the Provider and generally know how you are doing.

- **Individuals Involved in Your Care or Payment for Your Care.** We may release medical information about you to a friend or family member who is involved in your medical care and we may also give information to someone who helps pay for your care, unless you object in writing and ask us not to provide this information to specific individuals. In addition, we may disclose medical information about you to an entity assisting in a disaster relief effort so that your family can be notified about your condition, status and location.

- **Research.** Under certain circumstances, we may use and disclose medical information about you for research purposes. For example, a research project may involve comparing the health and recovery of all patients who received one medication to those who received another, for the same condition. All research projects, however, are subject to a special approval process. This process evaluates a proposed research project and its use of medical information, trying to balance the research needs with patients' need for privacy of their medical information. Before we use or disclose medical information for research, the project will have been approved through this research approval process, but we may, however, disclose medical information about you to people preparing to conduct a research project, for example, to help them look for patients with specific medical needs, so long as the medical information they review does not leave the Provider. We will almost always generally ask for your specific permission if the researcher will have access to your name, address or other information that reveals who you are, or will be involved in your care at the Provider.

- **As Required By Law.** We will disclose medical information about you when required to do so by federal, state or local law.

- **To Avert a Serious Threat to Health or Safety.** We may use and disclose medical information about you when necessary to prevent a serious threat to your health and safety or the health and safety of the public or another person. Any disclosure, however, would only be to someone able to help prevent the threat.

- **Email Use.**
  Email will only be used following this Organization's current policies and practices and with your permission. The use of secured, encrypted e-mail is encouraged.

Section D: Special Situations

- **Organ and Tissue Donation.** If you are an organ donor, we may release medical information to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation.

- **Military and Veterans.** If you are a member of the armed forces, we may release medical information about you as required by military command authorities. We may also release medical information about foreign military personnel to the appropriate foreign military authority.

- **Workers' Compensation.** We may release medical information about you for workers' compensation or similar programs.

- **Public Health Risks.** We may disclose medical information about you for public health activities. These activities generally include the following:
  - to prevent or control disease, injury or disability;
  - to report births and deaths;
  - to report child abuse or neglect;
  - to report reactions to medications or problems with products;
  - to notify people of recalls of products they may be using;
  - to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition; and
  - to notify the appropriate government authority if we believe a patient has been the victim of abuse, neglect or domestic violence. We will only make this disclosure if you agree or when required or authorized by law.

- **Health Oversight Activities.** We may disclose medical information to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.

- **Lawsuits and Disputes.** If you are involved in a lawsuit or a dispute, we may disclose medical information about you in response to a court or administrative order. We may also disclose medical information about you in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.

- **Law Enforcement.** We may release medical information if asked to do so by a law enforcement official:

- in response to a court order, subpoena, warrant, summons or similar process;
- to identify or locate a suspect, fugitive, material witness, or missing person;
- about the victim of a crime if, under certain limited circumstances, we are unable to obtain the person's agreement;
- about a death we believe may be the result of criminal conduct;
- about criminal conduct at the Provider; and
- in emergency circumstances, to report a crime; the location of the crime or victims; or the identity, description or location of the person who committed the crime.

- **Coroners, Medical Examiners and Funeral Directors.** We may release medical information to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. We may also release medical information about patients of the Provider to funeral directors as necessary to carry out their duties.

- **National Security and Intelligence Activities.** We may release medical information about you to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

- **Protective Services for the President and Others.** We may disclose medical information about you to authorized federal officials so they may provide protection to the President, other authorized persons or foreign heads of state or conduct special investigations.

- **Inmates.** If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release medical information about you to the correctional institution or law enforcement official. This release would be necessary for the institution to provide you with health care, to protect your health and safety or the health and safety of others, or for the safety and security of the correctional institution.

Section E: Your Rights Regarding Medical Information about You

You have the following rights regarding medical information we maintain about you:

- **Right to Access, Inspect and Copy.** You have the right to access, inspect and copy the medical information that may be used to make decisions about your care, with a few exceptions. Usually, this includes medical and billing records, but may not include psychotherapy notes. If you request a copy of the information, we may charge a fee for the costs of copying, mailing or other supplies associated with your request.

- We may deny your request to inspect and copy medical information in certain very limited circumstances. If you are denied access to medical information, in some cases, you may request that the denial be reviewed. Another licensed health care professional chosen by the Provider will review your request and the denial. The person conducting the review will not be the person who denied your request. We will comply with the outcome of the review.

- **Right to Amend.** If you feel that medical information we have about you is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for as long as the information is kept by or for the Provider. In addition, you must provide a reason that supports your request.

- We may deny your request for an amendment if it is not in writing or does not include a reason to support the request. In addition, we may deny your request if you ask us to amend information that:
    - Was not created by us, unless the person or entity that created the information is no longer available to make the amendment;
    - Is not part of the medical information kept by or for the Provider;
    - Is not part of the information which you would be permitted to inspect and copy; or
    - Is accurate and complete.

- **Right to an Accounting of Disclosures.** You have the right to request an 'Accounting of Disclosures'. This is a list of the disclosures we made of medical information about you. Your request must state a time period which may not be longer than six years and may not include dates before April 14, 2003. Your request should indicate in what form you want the accounting (for example, on paper or electronically, if available). The first accounting you request within a 12 month period will be complimentary. For additional lists, we may charge you for the costs of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

- **Right to Request Restrictions.** You have the right to request a restriction or limitation on the medical information we use or disclose about you for payment or healthcare operations. You also have the right to request a limit on the medical information we disclose about you to someone who is involved in your care or the payment for your care, like a family member or friend. For example, you could ask that we not use or disclose information about a surgery you had. In your request, you must tell us what information you want to limit, whether you want to limit our use, disclosure or both, and to whom you want the limits to apply (for example, disclosures to your spouse). We are not required to agree to these types of request. We will not comply with any requests to restrict use or access of your medical information for treatment purposes.

You also have the right to restrict use and disclosure of your medical information about a service or item for which you have paid out of pocket, for payment (i.e. health plans) and operational (but not treatment) purposes, if you have completely paid your bill for this item or service. We will not accept your request for this type of restriction until you have completely paid your bill (zero balance) for this item or service. We are not required to notify other healthcare providers of these restrictions, that is your responsibility.

- **Right to Receive Notice of a Breach.** We are required to notify you by first class mail or by email (if you have indicated a preference to receive information by email), of any breaches of Unsecured Protected Health Information as soon as possible, but in any event, no later than 60 days following the discovery of the breach. "Unsecured Protected Health Information" is information that is not secured through the use of a technology or methodology identified by the Secretary of the U.S. Department of Health and Human Services to render the Protected Health Information unusable, unreadable, and undecipherable to unauthorized users. The notice is required to

include the following information:

- a brief description of the breach, including the date of the breach and the date of its discovery, if known;
- a description of the type of Unsecured Protected Health Information involved in the breach;
- steps you should take to protect yourself from potential harm resulting from the breach;
- a brief description of actions we are taking to investigate the breach, mitigate losses, and protect against further breaches;
- contact information, including a toll-free telephone number, e-mail address, Web site or postal address to permit you to ask questions or obtain additional Information.

In the event the breach involves 10 or more patients whose contact information is out of date we will post a notice of the breach on the home page of our website or in a major print or broadcast media. If the breach involves more than 500 patients in the state or jurisdiction, we will send notices to prominent media outlets. If the breach involves more than 500 patients, we are required to immediately notify the Secretary. We also are required to submit an annual report to the Secretary of a breach that involved less than 500 patients during the year and will maintain a written log of breaches involving less than 500 patients.

- **Right to Request Confidential Communications.** You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we only contact you at work or hard copy or e-mail. We will not ask you the reason for your request. We will accommodate all reasonable requests. Your request must specify how or where you wish to be contacted.

- **Right to a Paper Copy of This Notice.** You have the right to a paper copy of this Notice. You may ask us to give you a copy of this Notice at any time. Even if you have agreed to receive this Notice electronically, you are still entitled to a paper copy of this Notice. You may obtain a copy of this Notice at our website. n/a

To exercise the above rights, please contact the individual listed at the top of this Notice to obtain a copy of the relevant form you will need to complete to make your request.

Section F: Changes to This Notice

We reserve the right to change this Notice. We reserve the right to make the revised or changed Notice effective for medical information we already have about you as well as any information we receive in the future. We will post a copy of the current Notice. The Notice will contain on the first page, in the top right hand corner, the effective date. In addition, each time you register at or are admitted to the Provider for treatment or health care services as an inpatient or outpatient, we will offer you a copy of the current Notice in effect.

Section G: Complaints

If you believe your privacy rights have been violated, you may file a complaint with the Provider or with the Secretary of the Department of Health and Human Services;

http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html

To file a complaint with the Provider, contact the individual listed on the first page of this Notice. All complaints must be submitted in writing. You will not be penalized for filing a complaint.

Section H: Other Uses of Medical Information

Other uses and disclosures of medical information not covered by this Notice or the laws that apply to us will be made only with your written permission. If you provide us permission to use or disclose medical information about you, you may revoke that permission, in writing, at any time. If you revoke your permission, we will no longer use or disclose medical information about you for the reasons covered by your written authorization. You understand that we are unable to take back any disclosures we have already made with your permission, and that we are required to retain our records of the care that we provided to you.

Section I: Organized Healthcare Arrangement

The Provider, the independent contractor members of its Medical Staff (including your physician), and other healthcare providers affiliated with the Provider have agreed, as permitted by law, to share your health information among themselves for purposes of treatment, payment or health care operations. This enables us to better address your healthcare needs.

Digital Copier and Device Privacy

A. Coverage

Rafael Rivera Jr DDS PLLC (hereafter referred to as the 'Organization') workforce members (i.e. employees, contractors and volunteers) who utilize digital printers, photocopiers, scanners or other medical devices with internal hard drives or memory.

B. Create / Revision Date

2/3/2016

C. Purpose

To define guidelines for managing digital devices with the intent to prevent Protected Health Information (PHI) breach and / or HIPAA violations arising from PHI storage on the hard disk drives or memory of these digital devices.

D. Policy

The Organization has adopted this policy to ensure that PHI is not wrongfully disclosed by way of stored images or data memory within digital copiers, printers, scanners, medical devices, and fax machines.

Since 2002, most digital printers, photocopiers, scanners and fax machines have been manufactured to operate with an internal hard drive or memory that captures images of every document processed. Safeguards to protect information on these devices must be followed to prevent possible HIPAA violations and/or breaches caused by theft, unauthorized access, use, or disclosure; improper modification or destruction of data.

As a general rule, the Organization requires all copier, scanner and medical device companies to sign Business Associate Agreements and acknowledge that their technicians are trained on secure management of PHI.

E. Procedures

Information security policies and safeguards for protecting data stored on digital copiers and other devices may include the use of automated software routines that wipe clean any stored images on a routine basis. NOTE: NIST 800-66 guidance for destruction must be followed. Other mechanisms for securing data may include the use of passcodes or encryption of all images on these disks. Again, NIST 800-66 encryption guidelines should be utilized to create *secured PHI* or destruction of stored images by technicians on scheduled or on-demand basis.

Procedures for new equipment procurement

a. When buying or leasing new equipment, investigate and evaluate manufacturer

options for securing data on digital devices. Ensure that sales representatives selling/leasing the equipment are aware of the Organization's security concerns and requirements.

b. Procure software or other mechanisms that, ideally, destroy or encrypt according to NIST 800-66 guidelines (creating *secured PHI)* stored images immediately after each use or on a set basis, such as daily.
c. Set-up routine maintenance procedures to investigate whether or not this image destruction is occurring.

For existing equipment (already purchased)

a . Investigate with the vendor of the product the status of stored images and hard drives within each copier, scanner and medical device.
b . Determine if auto destruction or encryption routines are available for each unit and institute if possible.
c . Ensure that routine and on demand maintenance visits by technicians address this issue.
d . Never allow any equipment that may have hard drives to leave the premises without ensuring that all stored images have been destroyed or encrypted.

Equipment that is to be sold, traded, or disposed of

a. Determine the hard drive and stored image status of any machines to be sold, traded or disposed of before they leave the Organization property.
b. Ensure any hard drives are completely scrubbed clean (preferably according to NIST 800-66 destruction guidelines) prior to leaving the Organization's property.
c. Hard drives may be crushed or rendered unusable through certified destruction as an alternative to scrubbing.

F. References

- Stericycle Online Security Risk Assessment tool (SRA)
- Omnibus Final Rules
- (SRA) Line Item: C.25
- List additional references: n/a

HHS, OCR or Other Regulatory Investigations

A. Coverage

Rafael Rivera Jr DDS PLLC (hereafter referred to as the 'Organization') workforce members who access, use, disclose or transmit confidential patient information. Our workforce includes all clinical providers, clinical support staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

B. Create / Revision Date

2/3/2016

C. Purpose

The purpose of this policy is to provide guidance on managing investigations from HHS (Health and Human Services) Office for Civil Rights (OCR) or other privacy and / or security regulators and enforcement agencies.

D. Policy

It is the policy of this Organization to fully comply with HIPAA law and with all HIPAA-related investigations conducted by HHS, OCR or other regulatory bodies. And to not impede or obstruct any HIPAA privacy / security related investigations conducted by one of these agencies. Also to provide all documentation or assistance required by law or regulation in connection with any HIPAA related investigations conducted by one of these agencies.

The Office for Civil Rights (OCR) enforces HIPAA Privacy and Security violations and may act from complaints filed by individuals or upon internally generated Audits. Remember that OCR-initiated actions are from the United States Federal venue and are to be taken very seriously. Rules of procedure, response dates and formats are to be followed to the letter.

HHS / OCR investigations for Privacy and Security should trigger litigation response processes, with Legal Counsel involvement if the risk is deemed at a level to warrant their involvement. Litigation Response procedures should work to keep the records in question (and their associated meta-data) secure while also preventing spoliation of evidence (unauthorized withholding, hiding, altering, or destroying).

OCR will notify the Covered Entity (CE) via letter when an allegation of a HIPAA violation is issued. To the extent practical, OCR will seek the cooperation of the CE to informally resolve complaints. For example, OCR can provide technical assistance to help a covered entity voluntarily comply with the Privacy and Security Rules.

A CE has the right to respond to an allegation by submitting evidence to OCR indicating;

the alleged violation did not occur as described by the complainant; the action complied with Privacy and Security Rules; or the CE has taken prompt and effective action to correct the non-compliance. The last allegation response listed, taking corrective action, is very important to document in your response.

If the CE and OCR are unable to resolve the matter voluntarily, and if OCR's investigation results in a finding that the CE is not complying with the Privacy and Security Rules, HHS may initiate formal enforcement action which may result in the imposition of monetary penalties. Further, certain violations of Privacy and Security may result in criminal prosecution by the US Department of Justice. Penalties will vary significantly depending on factors such as the date of the violation, whether the CE knew or should have known of the failure to comply, or whether the CE's failure to comply was due to willful neglect. Penalties may not exceed a calendar year cap for multiple violations of the same requirement.

A penalty will not be imposed for violations in certain circumstances such as if:

- The failure to comply was not due to willful neglect and was corrected during a 30-day period after the entity knew or should have known the failure to comply had occurred (unless the period is extended at the discretion of OCR); or
- The Department of Justice has imposed a criminal penalty for failure to comply.
- A penalty may be reduced by OCR if the failure to comply was due reasonable cause and the penalty would be excessive given the nature and extent of the non-compliance.
- Before OCR imposes a penalty, it will notify the CE and provide the CE with an opportunity to provide written evidence of those circumstances that would reduce or bar a penalty. This evidence must be presented to OCR within 30 days of the notice. In addition if OCR states that it intends to impose a penalty, a CE has the right to request an administrative hearing to appeal the proposed penalty.

Sample Real-World OCR Data Request Addendum

The following questions have been included in OCR Privacy Investigations.

Sample Data Request Language from an OCR Letter

1. Please submit the additional documentation requested below to support the Organization's position. You will have 20 days from the date of the data request letter to submit the evidence.

2. Please state your internal Policies and Procedures regarding the use and disclosure of PHI pursuant to 45 C.F.R. §* 164.502 (a) and 164.502 (h). If said policy is in writing, please submit a copy of the internal document.

3. Please submit a copy of the Organization's internal safeguards, policies, and procedures that it has implemented pursuant to the Privacy Rule at 164.530(c). Indicate the dates of any redrafting of the policies since April 14, 2003.

4. Please state whether you conducted an internal investigation of the allegations contained in this complaint, if so, please submit a copy of your findings and state, in detail, any corrective action(s) taken by the Organization. If no corrective action was taken, please state the reason(s) why.

5. Please submit an access audit of Individuals Name electronic medical record showing which employees of the Organization accessed his records during Time Period.

6. Please submit an Accounting of Disclosures for Individuals Name designated record set pursuant to 45 C.F.R. § 164.528.

7. Please state whether the Organization has provided training to all members of its workforce on the Policies and Procedures with respect to PHI in compliance with 45 C.F.R. § 164.530 (b)(i) of the Privacy Rule.

8. Please submit a copy of the Organization's internal policies and/or procedures regarding sanctions against employees who violate any of the provisions of the Privacy Rule pursuant to 45 C.E.R. § 164.530 (e)(1), including, but not limited to, verbal or written reprimands, mandatory training, suspension, and/or termination.

9. Please state whether any employees were sanctioned by the Organization in compliance with 45 C.F.R. §164.530 (e)(l) due to the allegations contained in this complaint, including the date the sanction occurred and the type of sanction enacted. If no sanction occurred, please state the reason(s) why no employees were sanctioned.

10. Please outline steps you are willing to take resolve the situation described in the complaint (i.e. retraining employees, polish existing privacy policies, sanction the employees making the disclosures, etc.).

Additional possible sample language:

1. Submit a copy of the internal policies and/or procedures regarding sanctions against employees who violate any of the provisions of the Privacy Rule pursuant to 45 C.F.R. §
164.530 (e)(1), including, but not limited to, verbal or written reprimands, mandatory training, suspension, and/or termination.

2. Please state whether your company has provided training to all members of workforce on the policies and procedures with respect to protected health information in compliance with 45
C.F.R. § 164.530 (b)(1) of the Privacy Rule. Please specify the date of the last training and provide verification that your workforce received training

3. Please outline steps you are have taken and/or are willing to take resolve the situation described in the complaint (i.e. retraining employees, provide access to PHI, issue an apology letter, polish existing privacy policies,

sanction the employee(s) making the disclosures, etc.).

If an Investigation Is On-site

Workforce members who are designated to assist with these types of investigations conducted must adhere to the following:

- Cooperate, but do not volunteer information or records that are not requested.
  - Ask for the official government agency-issued identification of the investigators (Business cards are NOT official identification); write down their names, office addresses, telephone numbers, fax numbers and e-mail addresses. If investigators cannot produce acceptable I.D., call legal counsel immediately and defer the provision of any PHI until after you confer with counsel or until the investigators produce acceptable I.D. Ensure that you've made appropriate requests for I.D. and that they've been unreasonably refused before you do.)
- Have at least one, if not two witnesses available to testify as to your requests and their responses.
- Ask for the name and telephone number of the lead investigator's supervisor, but only if, in your judgment, his/her demeanor indicates that you can ask such a question without engendering "hard feelings." Under no circumstances should you take any action to escalate tensions, except if you genuinely doubt the identity or authority of the investigators.
- Determine if there are any law enforcement personnel present (i.e., FBI, US Attorney investigators, State Prosecutor investigators, etc.). If law enforcement personnel are present, then the investigation is likely a criminal one, with much more severe penalties than may result from a civil investigation.
- Permit the investigators to have access to protected health information ("PHI"), in accordance with the Organization's Notice of Privacy Practices ("NPP"), and Federal and State law. Once investigators have verified their identities and have also verified their authority to access PHI, it is a violation of HIPAA to withhold PHI from them, if the PHI sought is the subject matter of the investigation, or reasonably related to the investigation. Again, ask investigators to verify that they are seeking access to the information because it is directly related to their legitimate investigatory purposes; and document their responses in your own written records.
- Have a witness with you when you ask about their authority to access PHI, and the use that they will make of the PHI they are seeking access to, who can later testify as to what they told you. Two witnesses are even better. All witnesses should also prepare a written summary of the conduct and communications they observed as soon as possible after the incident; these summaries should be annotated with the time and date of the event, the time and date that the summaries were completed, and the witnesses signature.
- Send staff employees elsewhere, if possible, during this first investigation encounter. There is no requirement that the organization must provide witnesses to be questioned during the initial phase of an investigation.
- Do not instruct employees to hide or conceal facts, or otherwise mislead investigators.
- Ask the investigators for documents related to the investigation. For example, request:

    - Copies of any search warrants and/or entry and inspection orders
    - Copies of any complaints
    - A list of patients of interest
    - A list of documents/items seized
- Do not expect that investigators will provide any of the above, except for the search warrant and a list of documents/items seized (if any).
- Don't leave the investigators alone, if possible. Assign someone to "assist" each investigator present.
- Don't offer food (coffee, if already prepared, and water, if already available, is ok). Don't do anything that could be construed as a "bribe" or a "kickback" to induce favorable treatment, such as offering to buy the investigators lunch.
- Don't be "chatty." Only tell investigators what you are required by law to tell them. Answer direct questions fully and to the best of your ability. Always defer to the advice of legal counsel if you are unsure of what or how much to say.

Omnibus Enforcement Updates

- Enforcement provisions are very 'legal' in scope; consider involving legal counsel, especially if any there is possible willful neglect.
- OCR currently conducts a preliminary review of every complaint received and proceeds with the investigation in every eligible case where its preliminary review of the facts indicates a possible violation of the HIPAA Rules.
    - OCR will investigate any complaint filed under this section when a preliminary review of the facts indicates a possible violation due to willful neglect.
        - OCR would have continued discretion with respect to investigating any other complaints.
        - OCR may on a case-by-case basis expand the preliminary review and conduct additional inquiries for purposes of identifying a possible violation due to willful neglect.
        - Complaint investigations and compliance reviews clarify that OCR generally conducts compliance reviews to investigate allegations of violations of the HIPAA Rules brought to their attention through a mechanism other than a complaint.
        - Complaints or Compliance Reviews can be the basis of an investigation.
- Although OCR will encourage voluntary corrective action; enforcement can also skip right to civil or criminal penalties if they determine the need to, they are not required to work with the CEs / BAs for resolution rather than having to exhaust all informal efforts, especially for willful neglect.

Factors Considered in Determining the Amount of a Civil Money Penalty

- The general factors the Secretary of HHS will consider in determining a

CMP (Civil Monetary Penalty).
    - The nature and extent of the violation
        - Time period during which the violation(s) occurred and the number of individuals affected
        - The nature and extent of the harm resulting from the violation
    - The history of prior compliance with the HIPAA (and administrative simplification) including violations by the covered entity or business associate
    - The financial condition of the covered entity or business associate
    - Such other matters as justice may require.
- The facts of the situation will determine whether reputational harm has occurred, such as whether the unlawful disclosure resulted in adverse effects on employment, standing in the community, or personal relationships.
    - In determining the nature and extent of the harm involved, the Organization may consider all relevant factors, not just those expressly included in the text of the regulation.

E. Related Policies

- 7s - Confidentiality of PHI
- 21s - HIPAA Violation and Breach Reporting
- List additional related policies: n/a

F. References

- Sample OCR Communication alleging HIPAA Privacy non-compliance, received November 2009.
- OCR Privacy investigation letter from late 2009
- 45 C.F.R. Part 160 Administrative Simplification: Enforcement Interim Final Rule
- Omnibus Privacy Final Rule Modifications, January 2013
- Subtitle D of the HITECH Act, sections 13400–13424
- Sample OCR Communication alleging HIPAA Privacy non-compliance, received November 2009.
- OCR Privacy investigation letter from late 2009
- 45 C.F.R. § 164.528
- 45 C.F.R. § 164.502 (a) & 45 C.F.R. § 164.502 (h)
- 45 C.F.R. § 164.530(c)
- 45 C.F.R. § 164.530 (b)(i)
- 45 C.E.R. § 164.530 (e)(1)
- 45 C.F.R. §164.530 (e)(l)
- 45 C.F.R. § 164.308, § 164.310, and § 164.312, others
- Stericycle Online Security Risk Assessment (SRA)
- SRA Line Item Number: B9
- List additional related references: n/a