POLICY/PROCEDURE TITLE	Investigation and Mitigation of Privacy Breaches
POLICY/PROCEDURE NUMBER	CC-114
DEPARTMENT	Corporate Compliance Department
Original Issue Date	July 19, 2018
Next Scheduled Review Date	July 1, 2019
Last Review Date	July 19, 2018
Revision Date History	N/A
Author:	N/A
Approved by:	Corporate Compliance Committee

I. PURPOSE:

To set forth the policy and procedure of ReachOut Healthcare America, LTD d/b/a Smile America Partners (hereinafter "Smile America Partners") regarding the investigation and mitigation of Privacy Breaches.

II. SCOPE:

This policy is applicable to all reported, known or suspected instances of a privacy breach.

III. DEFINITIONS:

1. **Unsecured Protected Health Information** - PHI that has not been secured by a method specified by Department of Health and Human Services (DHHS) to render PHI unusable, unreadable or indecipherable to unauthorized persons.

2. **Breach** - Any acquisition, access, use or disclosure of PHI in violation of the Privacy Rule shall be presumed to be a "breach" (i.e., that it compromises the security or privacy of the PHI), unless the Chief Compliance Officer determines that one of the following exceptions applies:

    a. the acquisition, access or use of PHI was:

        (1) unintentional, and that it was made in good faith, and that it occurred within the scope of authority by a workforce member or person acting under the authority of Smile America Partners, or by a dental practice for whom Smile America Partners is the Administrator, or by a business associate, and the acquisition, access or use of PHI does not result in further use or disclosure in a manner not permitted by the Privacy Rule.

    b. the acquisition, access or use of PHI constitutes an inadvertent disclosure:

        (1) by a person who is authorized to access PHI at Smile America Partners, or by a dental practice for whom Smile America Partners is the Administrator, or by a business associate to another person who is authorized to access the subject PHI, and disclosed in a manner not permitted by the Privacy Rule.

(2) the Corporate Compliance Officer or his/her designee as directed has a good faith belief that the recipient(s) of the unauthorized disclosure of PHI could not have been able to retain such information.

(3) based on a risk assessment, the Corporate Compliance Officer or his/her designee as directed determines that there is a low probability that the PHI has been compromised.

3. **Covered Entity** – A Covered Entity is defined in the HIPAA rules and/or regulations as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards. Each dental practice for whom Smile America Partners serves as the Administrator is a Covered Entity.

IV. POLICY:

Smile America Partners takes seriously its role in ensuring the privacy and security of protected health information. Smile America Partners will follow the procedures described below for investigating any reported or suspected wrongful acquisition, access, use or disclosure of PHI and for responding to such incidents in accordance with legal requirements.

V. PROCEDURE:

1. The Chief Compliance Officer, and as appropriate the legal counsel, will investigate each reported or suspected violation and determine whether a violation has occurred. The investigation will include an assessment of the incident, notification to individuals and/or certain other persons or entities as required.

4. The Chief Compliance Officer or his/her designee as directed will conduct a risk assessment of any suspected or reported breach to ascertain whether there is a low probability that the PHI has been compromised and will take appropriate action to the nature of the violation. If necessary, the Chief Compliance Officer will consult with legal counsel to determine the proper response to a suspected privacy violation. The following factors will be considered in determining the appropriate response:

    a. the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

    b. the unauthorized persons who used the PHI or to whom the disclosure was made;

    c. whether the PHI was actually acquired or viewed; and

    d. the extent to which the risk to the PHI has been mitigated.

5. The Corporate Compliance Department will keep records of the examination and risk assessment and of notifications provided on file for a period of six years.

6. Whenever possible, the Chief Compliance Officer or his/her designee will contact the recipient of wrongfully disclosed PHI (if they can be identified) and notify them that the disclosure was in error. If written records were mistakenly disclosed, the Chief Compliance Officer or his/her designee will seek to have the records returned or destroyed by the recipient. The Chief Compliance Officer or his/her designee will send the recipient a Certificate of Destruction/Return and request that the Certificate be completed and returned to the Chief Compliance Officer or his/her designee.

7. The nature of the violation will determine the extent of the mitigation effort undertaken. Appropriate responses to a violation may include the following:

    a. notifying the Covered Entity in accordance with the Business Associate Agreement (see CC-116 Business Associate Agreements Policy);

    b. preparing the breach notification on behalf of the applicable Covered Entity;

    c. preparing the corrective action plan.

    d. re-training workforce members on the requirements of HIPAA and the importance of protecting PHI; and/or

    e. disciplining employees who are responsible for the violation, up to and including termination.

    The Covered Entity maintains ultimate authority and responsibility for reporting a breach to external agencies and to the individual(s)/personal representative of the individual(s) affected by the breach. The Chief Compliance Officer and staff will work collaboratively with the Covered Entity and Smile America Partners' Senior Management Team to ensure accurate findings, resolution and reporting.

8. Additional actions may occur, including but not limited to, revising policies and procedures and/or workforce training and/or other corrective action as may be identified to prevent similar future violations.