COMPLIANCE POLICY — The Smile Way Group

POLICY/PROCEDURE TITLE	Investigation, Mitigation and Reporting of HIPAA Privacy Breaches
POLICY/PROCEDURE NUMBER	CC-114
DEPARTMENT	Corporate Compliance Department
Original Issue Date	7/19/2018
Next Scheduled Review Date	06/26/2025
Last Review Date	07/10/2024
Revision Date History	1/2023 Revised organizational information to apply to The Smile Way Group, added HIPAA privacy breach reporting details; 3/2023 added SNYO and WA DPP; 2/2024 minor edit; 4/2024 added certificate; 7/2024 NYC DOE

APPLIES TO

☒	SAP: ReachOut Healthcare America Ltd. dba Smile America Partners	☒	MI: Michigan Dental Outreach, P.C. dba Michigan Dental Outreach
☒	AZ: Arizona Mobile Dental, PC dba Big Smiles	☒	MO: Nevin K. Waters D.D.S., P.C. dba Big Smiles
☒	CA: Elliot Paul Schlang, DDS, Professional Corporation dba Big Smiles	☒	NC: Theodore F. Mayer, DDS P.A. dba Smile North Carolina
☒	GA: Shurett Dental Group, P.C. dba Shurett Dental Group	☒	NY: Big Smiles Dental New York, PLLC
☒	GA: Mark Shurett, DDS, PC dba Help A Child Smile	☒	NY: Smile New York Outreach, LLC
☒	IL: Elliot P. Schlang, D.D.S. P.C. dba Smile Illinois	☒	OH: Elliot P. Schlang DDS, Dental Outreach PLLC dba Ohio Dental Outreach
☒	IN: Elliot P. Schlang DDS, Dental Outreach PLLC dba Indiana Dental Outreach	☒	PA: Big Smiles Pennsylvania P.C. dba Smile Pennsylvania
☒	KS: Nevin K. Waters D.D.S., PA dba Big Smiles	☒	UT: Big Smiles Utah, P.C. dba Big Smiles
☒	KY: Big Smiles Kentucky PSC dba Big Smiles	☒	VA: Big Smiles Virginia PC dba Smile Virginia
☒	MA: Elliot P. Schlang DDS Big Smiles Massachusetts P.C. dba Smile Massachusetts	☒	WA: Michael LaCorte Dentistry, PC dba Big Smiles
☒	MD: S.K. Pesis D.D.S., Big Smiles Maryland, PC dba Smile Maryland	☒	WV: Elliot P. Schlang DDS, Inc. dba Smile West Virginia

I. PURPOSE:

To set forth the policy and procedure of ReachOut Healthcare America, LTD d/b/a Smile America Partners (”SAP”) and its affiliated Dental Professional Practices (“DPPs”) (hereinafter collectively referred to as “The Smile Way Group”) regarding the investigation, mitigation of Privacy Breaches and addressing applicable state and federal laws and regulations governing notice to affected persons in the event of a breach of patient privacy.

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:

        i. 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 The Smile Way

Group, 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:

i. by a person who is authorized to access PHI at The Smile Way Group, 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.

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

iii. 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 DPP for whom SAP serves as the Administrator is a Covered Entity.

IV. POLICY:

The Smile Way Group takes seriously its role in ensuring the privacy and security of protected health information. The Smile Way Group 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.

2. 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.

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

4. 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 (Addendum A) and request that the Certificate be completed and returned to the Chief Compliance Officer or his/her designee.

5. 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.

    f. notifying the insurance carrier

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 to ensure accurate findings, resolution and reporting.

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.

VI. BREACH NOTIFICATION REQUIREMENTS:

Following a breach of unsecured protected health information, the Chief Compliance Officer must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

1. Individual Notices: Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. The notice shall include to the extent possible: (1) a brief description of what happened (e.g., the date(s) of the breach and its discovery); (2) a description of the types of information affected (e.g., whether the breach involved names, social security numbers, birthdates, addresses, diagnoses, etc.); (3) steps that affected patients should take to protect themselves from potential harm resulting from the breach; (4) a brief description of what PROVIDER is doing to investigate, mitigate, and protect against further harm or breaches; and (5) contact procedures for affected persons to ask questions and receive information, which shall include a toll-free telephone number, e-mail address, website, or postal address at which the person may obtain more information. The notice shall be written in plain language. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside. The covered entity must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written notice, by telephone, or other means. These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity (or business associate, as applicable).With respect to a breach at or by a business associate, while the covered entity is ultimately responsible for ensuring individuals are notified, the covered entity may delegate the responsibility of providing individual notices to the business associate. Covered entities and business associates should consider which entity is in the best position to provide notice

to the individual, which may depend on various circumstances, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual.

2. Media Notice: Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

3. Notice to the HHS: If the Chief Compliance Officer determines that a breach of protected health information has occurred, the Chief Compliance Officer shall also notify HHS of the breach as described below. Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.

VII. BREACH NOTIFICATION REQUIREMENTS OF NYC BOARD OF EDUCATION:

The Processor shall promptly notify, without unreasonable delay (a) the BOE Office of Legal Services at 212-374-6888 and at studentprivacy@schools.nyc.gov (to the attention of the Chief Privacy Officer) and (b) the BOE Division of Information and Instructional Technology at data-security@schools.nyc.gov (to the attention of the Chief Information Security Officer) of: (i) any unauthorized release or other Processing of Confidential Information, whether by the Processor, its Authorized Users or any other party that shall have gained access to the affected Confidential Information, or any other Security Incident; or (ii) any other breach of contractual obligations relating to data privacy and security under this Agreement or any other applicable Agreement (together with a Security Incident, a "Reportable Data Event").

In no event shall such notification occur more than twenty four (24) hours after confirmation of an event described in clause (i) of the previous sentence, or more than seventy-two (72) hours after confirmation of an event described in clause (ii) of the previous sentence.

Such notification of the DOE shall summarize, in reasonable detail, the nature and scope of the Security Incident (including a description of all impacted DOE Data and DOE Technology Assets) and the corrective action already taken or planned by Processor, which shall be timely supplemented to the level of detail reasonably requested by the BOE, inclusive of relevant investigation or forensic reports.

To the extent both (a) New York Education Law 2-d or any other law or regulation requires Subjects affected by the Reportable Data Event to be notified, and (b) the Reportable Data Event is not exclusively attributable to the acts or omissions of the BOE, the Processor shall be responsible, at its own cost and expense, to notify in writing all persons affected by the Reportable Data Event, or shall compensate the BOE for the full cost of any notifications that the BOE instead makes.

The Processor agrees to assist and collaborate with the BOE in ensuring that required notifications shall be clear, concise, use language that is plain and easy to understand, and to the extent available, include: (a) a brief description of the Reportable Data Event, the dates of the incident and the date of discovery, if known; (b) a description of the types of Confidential Information affected; (c) an estimate of the number of records affected; (d) a brief description of the investigation or plan to investigate; and (e) contact information for representatives who can assist parents or adult students that have additional questions.

If requested, Processor shall provide the BOE with (a) physical access to the affected locations and operations within the control of Processor; (b) access to Processor's Authorized Users or other individuals with knowledge of the Reportable Data Event.

The Processor shall fully cooperate with and assist the BOE in investigating the Reportable Data Event or in effectuating notifications, including, without limitation, by providing full access to any information, records or other material the BOE deems to be necessary for such purposes or required to comply with applicable law.

VIII. NOTIFICATION BY A BUSINESS ASSOCIATE:

Business Associate: If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the Chief Compliance Officer following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any other available information required to be provided by the covered entity in its notification to affected individuals.

IX. ADMINISTRATIVE REQUIREMENTS AND BURDEN OF PROOF:

1. Covered entities and business associates, as applicable, have the burden of demonstrating that all required notifications have been provided or that a use or disclosure of unsecured protected health information did not constitute a breach. Thus, with respect to an impermissible use or disclosure, a covered entity (or business associate) should maintain documentation that all required notifications were made, or, alternatively, documentation to demonstrate that notification was not required: (1) its risk assessment demonstrating a low probability that the protected health information has been compromised by the impermissible use or disclosure; or (2) the application of any other exceptions to the definition of "breach."
2. Covered entities are also required to comply with certain administrative requirements with respect to breach notification. For example, covered entities must have in place written policies and procedures regarding breach notification, must train employees on these policies and procedures, and must develop and apply appropriate sanctions against workforce members who do not comply with these policies and procedures.

IX. DOCUMENTATION:

The Chief Compliance Officer or their designee may prepare and maintain documentation required by this policy for a minimum period of six (6) years, including but not limited to reports or complaints of privacy violations; results of investigations, including facts and conclusions relating to the risk assessment; required notices; logs of privacy breaches to submit to HHS; sanctions imposed; etc.

Approvals:

DocuSigned by:
Steve Higginbotham 7/23/2024
9F2E17E4D88A41A...
Steve Higginbotham, CEO

DocuSigned by:
Craig Thomas 7/23/2024
068E7D1B7A624EC...
Craig Thomas, CCO & SVP HR

Addendum A: Certification of Destruction / Return Form Sample

CERTIFICATION OF DESTRUCTION / RETURN FORM

By completing this form, you are acknowledging that you have received and viewed correspondence for a patient not at the address listed or with whom you have no current affiliation. If you have questions, please contact Krista Malinich at 888-833-8441 x 60142.

Section A: Who is the receiver of this information?

Name: _____

Section B: Check all that apply and complete

- ☐ I have enclosed the misdirected letter or written correspondence meant for patient _____.
- ☐ I no longer have the misdirected letter or written correspondence in possession.
  - ☐ I have already thrown away the correspondence.
  - ☐ I have already shredded/destroyed the correspondence.

_____ _____

Signature Date:

Please return this form with the misdirected letter or written correspondence if availabiltiy to the administrative office as soon as possible. Thank you!

Big Smiles Help A Child Smile Mobile Dental Program Shurett Dental Group Family Dentistry Smile Programs ...the mobile dentists

Administration Office 33533 W 12 Mile Road, Suite 150, Farmington Hills, MI 48331-9912