COMPLIANCE POLICY — The Smile Way Group

POLICY/PROCEDURE TITLE	Computer and Information Security Policy
POLICY/PROCEDURE NUMBER	CC-118
DEPARTMENT	Corporate Compliance Department
Original Issue Date	8/16/2018
Next Scheduled Review Date	4/24/2025
Last Review Date	4/25/2024
Revision Date History	10/2022 policy updated to include DPP and The Smile Way Group, title changed from "Clean Workstation", remote and field sections added; 3/2023 added SNYO and WA DPP; 4/2024 edits.

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:

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") has established this policy for the purpose of improving the security and confidentiality of information, including but not limited to Protected Health Information ("PHI"). This policy ensures that all PHI and any other sensitive and confidential information, whether it be on paper, a storage device, or a hardware device, is properly locked away or disposed of when a workstation is not in use. This policy will reduce the risk of unauthorized access to, loss of, and damage to information during and outside of normal business hours or when workstations are left unattended. A Computer and Information Security Policy is an important HIPAA security and privacy control.

II. SCOPE:

This policy applies to all individuals of The Smile Way Group working with PHI or any other sensitive and confidential information in any form (hardcopy or electronic).

III. POLICY:

Office Staff:

- Passwords may not be left on sticky notes posted on or under a computer, or left written down in an accessible location.
- Computer workstations must be locked when the workstation is unoccupied and should be configured to automatically lock or engage password protected screensaver after an unattended duration of 10 minutes.

- Laptops, tablets, cell phones, and other portable computing devices must also be locked when not in use or when unattended.
- Computer workstations must be logged off at the end of the workday.
- Individuals are required to ensure that any sensitive and confidential information in hardcopy or electronic form is removed from their workstations and locked when their workstations are unoccupied and at the end of the workday.
- Storage devices such as CDs, DVDs, hard drives, and USB drives containing any sensitive and confidential information must be locked in a drawer, and data contained therein must be encrypted.
- File cabinets containing any sensitive and confidential information must be kept closed and locked when not in use or when unattended.
- Keys used for access to any sensitive and confidential information must not be left at an unattended desk.
- Printouts containing any sensitive and confidential information should be immediately removed from the printer/copiers. Unclaimed printouts/faxes should be placed in the corresponding folders so PHI is protected from casual viewing. Individuals must ensure that no documents containing any sensitive and confidential information remain in the printer/copier areas overnight. Staff that routinely prints sensitive and confidential information should contact IT to see if secure print mode is available on their printer.
- Upon disposal, any sensitive and confidential information must be shredded.
- Whiteboards containing any sensitive and confidential information must be erased.

Remote Office Staff:

- Passwords may not be left on sticky notes posted on or under a computer, or left written down in an accessible location.
- Computer screens must be faced away from any nonemployee when in use, and when not in use, devices must remain locked.
- Workstations should be configured to automatically lock or engage password protected screensaver after an unattended duration of 10 minutes.
- Laptops, tablets, cell phones, and other portable computing devices must also be locked when not in use or when unattended.
- Computer workstations must be logged off at the end of the workday.
- Individuals are required to ensure that any sensitive and confidential information in hardcopy or electronic form is secure when their workstation is unoccupied and at the end of the workday.
- With prior IT departmental approval, any storage devices such as CDs, DVDs, hard drives, and USB drives containing any sensitive and confidential information must be stored securely, and data contained therein must be encrypted.
- Printouts containing any sensitive and confidential information should be immediately removed from the company issued printer/copiers. Individuals must ensure that no documents containing any sensitive and confidential information remain in the printer/copier areas overnight.
- Upon disposal, any sensitive and confidential information must be shredded or returned to the office for shredding.

Field Staff:

- Passwords may not be left on sticky notes posted on or under a computer, or left written down in an accessible location.
- At no time should dental equipment or sensitive and confidential information be left unattended while at school visit. Sensitive and confidential information may not be stored overnight in vehicles.
- Upon disposal, any sensitive and confidential information must be shredded. If a shredder is not available, it should be included in the weekly mailing to the corporate office with a “SHRED” note on it.
- Computer workstations must be locked when the workstation is unoccupied and should be configured to automatically lock or engage password protected screensaver after an unattended duration of 10 minutes.
- Any other company issued portable computing devices, such as laptops, tablets, cell phones, must also be locked when not in use or when unattended.
- Computer workstations must be logged off at the end of the workday.

- **Team Leaders:** Storage devices such as CDs, DVDs, hard drives, and USB drives containing any sensitive and confidential information must be secure when not in use, and data contained therein must be encrypted. These may not be stored overnight in vehicles.
- **Team Leaders:** Printouts containing any sensitive and confidential information should be immediately removed from the company issued printer/copiers and secured appropriately.

IV. ENFORCEMENT:

Individuals found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Approvals:

DocuSigned by:
Steve Higginbotham 7/23/2024
9E2E17E4D88A41A...
Steve Higginbotham, CEO

DocuSigned by:
Craig Thomas 7/23/2024
968E7D1B7A624EC...
Craig Thomas, CCO & SVP HR