
Privacy & Security Guidelines

Clinical Training for School Dental Sealant Programs
Tuesday, August 11, 2020



Privacy & Security

- Clients (schools and parents/guardians) expect that their medical/dental records and data will be kept safe and secure.
- School dental sealant programs have a legal responsibility to secure any confidential information related to a patient (such as names, dates, services provided, and medications).
 - Health Insurance Portability & Accountability Act (HIPAA)
 - Family Educational Rights and Privacy Act (FERPA)

HIPAA

- Requires the protection and confidential handling of protected health information (verbal, written, electronic).
- Requires covered entities to establish policies and practices that ensure protected health information (PHI) is protected and secure.
- Protected health information (PHI) – any health-related information that can be used alone, or in combination with other info., to identify an individual.
 - Names of individuals and relatives
 - Mailing and E-mail addresses
 - Health plan beneficiary numbers

HIPAA

- PHI can only be used and disclosed – *to the minimum necessary* – for treatment, payment, and healthcare operations purposes.
 - Minimum necessary standard requires organizations to evaluate their practices and enhance safeguards to:
 - Limit unauthorized or inappropriate access to PHI
 - Limit unauthorized disclosures of PHI

Once a disclosure is made, it is too late to get it back.

HIPAA Privacy Rule During Emergencies

- It is essential for covered entities to notify public health authorities of a COVID-19 infected patient, as the public health authorities will need information in order to ensure public health and safety.
- It is permissible to share PHI with public health authorities such as the CDC, state and local health departments, and others responsible for ensuring the safety of the public.
- In such cases PHI may be shared without obtaining authorization from the patient.

FERPA Regulations

- FERPA protects the privacy of student education records which are directly related to a student and maintained by an institution or a party acting for the institution.
- FERPA applies to personally identifiable information in educational records:
 - Student's name
 - Names of family members
 - Addresses
 - Personal identifiers (mother's maiden name, **student ID number**, social security number etc.)

FERPA Regulations

- A school may disclose “directory information” without consent if the school has adopted directory information policies to disclose properly designated directory information without consent on students whose parents have not opted out of the disclosure of directory information.
- “Directory information” means information in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed.
 - Name, address, grade level, etc.

Examples of Security Incidents

- Unsecured Networks – accessing a network that does not have security protections (e.g. Starbucks).
- E-mail Errors – sending sensitive information to the wrong person.
- Unattended Computer/Laptop/iPad – leaving a computer logged on and unattended.
- Passwords – leaving passwords in plain view of others.
- Misplaced Health Insurance Info – misplaced document containing health insurance information.

Working in Public Spaces

- **Shoulder Surfing:** Refers to looking over someone's shoulder to obtain information. It commonly occurs in busy environments, such as an office or hotel lobby.
- **Eavesdropping:** Occurs when someone secretly listens in on a conversation.
- **Unsecured Mobile Devices:** Mobile devices—such as laptops, mobile phones, and USB flash drives—are vulnerable to theft and unauthorized access if they are left unattended and unsecured.

Securing Work Areas

- Don't leave sensitive information in plain view. A cluttered workspace often leaves sensitive information in plain view.
- Don't throw away sensitive information in an unsecured waste bin. Thieves look for information in our trash, and the loss of information can result in a privacy breach.
- Don't delay in retrieving sensitive information. Promptly retrieve documents from printers or fax machines, and clean whiteboards after use.

Access Controls

- Never let anyone – even someone you recognize – follow you into a secured area without first seeing credentials from the school.
- Never prop open a door to a secured area. Doing so defeats the purpose of access controls for preventing unauthorized entry.
- Never assume you know the access privileges of others. Visitors may not be authorized to access the same areas as you.

ODE Guidance on Volunteers & Visitors

- Volunteers and visitors should be limited, to the greatest extent possible, from on-site activities.
- Staff members (e.g. substitute teachers, district staff who move between buildings), contracted service providers (e.g. counseling services, maintenance), and partner providers (e.g. student teachers, DHS Child Protective Services staff) are not considered visitors or volunteers.
 - School dental sealant programs are considered visitors.

ODE Guidance on Visitors & Volunteers

- Schools must:
 - **Restrict non-essential visitors/volunteers.**
 - Screen all visitors/volunteers for symptoms upon every entry. Restrict from school property any visitor known to have been exposed to COVID-19 within the preceding 14 calendar days.
 - Visitors/volunteers must wash or sanitize their hands upon entry and exit.
 - Visitors/volunteers must maintain six-foot distancing, wear face coverings, and adhere to all other provisions of this guidance.

Tailgating

- Holding the door open for another person seems like common courtesy, but the threat of theft, property damage, or even violence within a school makes this a potential security risk.
- You need to do your part in preventing unauthorized entry and reporting any “tailgating” incidents to the front office right away.

Example of Tailgating

You hear a knock at the classroom door. Outside in the hallway is a person wearing overalls and carrying an electrician's toolkit. They say, "Hi. Someone called me out to do some maintenance to the air conditioning unit in the classroom."

- How would you respond to this scenario?

Suggested Response: "Who was it that called you so I can confirm and get you started?"

Always confirm a third-party's legitimacy by checking with staff from the front office.

Is it Safe or Risky?

Electronic Safeguards

1. Deactivate your computer's system security and firewall when connected to your corporate network.
 - Risky
2. Download unauthorized software or files to increase your productivity.
 - Risky
3. Install updates to your system as soon as they arrive from your IT department.
 - Safe

Is it Safe or Risky?

Passwords

1. Use the same, easy to remember password, for all logins.
 - Risky
2. Create a strong password including a variety of characters.
 - Safe
3. Set your screensaver to unlock with a password.
 - Safe
4. Share your password only with your IT department.
 - Risky – never share your password

Is it Safe or Risky?

Electronic Communication

1. Encrypt personal information to prevent unauthorized access.
 - Safe
2. Share personal information only with those that have a "need-to-know."
 - Safe
3. Include personal information in the subject line of e-mails.
 - Risky

Is it Safe or Risky?

Physical Documents

1. Dispose of parent permission forms and USB drives containing PHI in the trash at home or office.
 - Risky – use a secure shred container
2. Lock documents or files containing protected information in a secure place, such as a locker or vehicle trunk.
 - Safe
3. Print e-mails containing protected information to create a paper-trail if future access is needed.
 - Risky

Is it Safe or Risky?

Access Controls

1. Never hold the door open for "tailgaters" who do not have credentials.
 - Safe
2. Lock your laptop/iPad when leaving it unattended, even for short periods.
 - Risky – take your computer/iPad with you at all times unless the room can be secured
3. Allow visitors to move through the building without an escort.
 - Risky

Privacy & Security In Practice

- Distribute HIPAA forms (i.e. notice of privacy practices) along with parent/guardian permission forms.
- COVID-19 considerations when collecting client-level data, either in paper or electronic format:
 - Add special fields (i.e. temperature reading)
 - Implement procedures for disinfecting computers, laptops, iPads, etc.

Privacy & Security In Practice

- Client-level data, either in paper or electronic format, should be secured at all times:
 - When in transit to a school or home, securely lock completed forms or an iPad/laptop in a vehicle trunk or hidden from sight.
 - Hide completed forms from sight or take the iPad/laptop with you during breaks and at lunchtime.
 - Store completed forms and technology at home or in a hotel room overnight.
 - Use tamper resistant envelopes.

Security of Electronic Data

- Encrypt your data
- Use strong passwords
- Secure your network
 - Use only secure Wi-Fi networks and not public networks (e.g. Starbucks).
 - When syncing data from the field, ensure the data is encrypted during transmission.
 - Third party host may be needed to get past a firewall.
- Use antivirus software

Questions?