Information Privacy and School Dental Sealants Programs

Corinna Brower MPH, BSN, RN
State School Nurse Consultant
Adolescent and School Health Programs
Public Health Division, Oregon Health Authority

Oregon Health Authority

Privacy & Security

- Clients (students, parents/guardians) expect that their medical/dental records and data will be kept private and safe.
- School dental sealant programs have a legal and ethical responsibility to secure any confidential information related to a patient (such as names, dates, services provided, and medications).

Oregon Health Authority

Could this be a privacy violation?

Student: “Why did my friend get a happy face on their paper and I got a sad face?”

School administrator: “I’ll need the list of which students were screened today.”

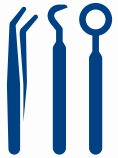
Parent: “Thanks for letting me into the treatment space. I see my neighbor’s kid getting treated. Can I get a copy of the notes? I’ll drop them off this afternoon.”

Who needs dental records?

- Dental clinics, DCOs, sealant program providers ?
- Families / students ?
- Schools / districts ?

Oregon Health Authority

Who needs dental records?



- Dental clinics, DCOs, sealant program providers
  - Records per facility/employer protocols
- Families/students
  - Treatment record, referral information
- Schools/districts
  - Care coordination *if provider has permission to share information*
  - ODE does not collect dental *sealants* data
  - ODE collects dental *screening* data
    - School districts are required to collect information about *whether dental screening was completed* for new students age 7 and younger [HB 2972]

Oregon Health Authority

What regulates information sharing?

HIPAA: Health Insurance Portability & Accountability Act

FERPA: Family Educational Rights and Privacy Act

Local protocols must align with federal privacy laws.

Both laws require protection of identifiable information

- Key differences in permissible sharing

Oregon Health Authority

HIPAA

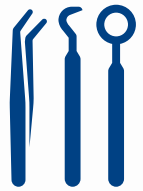
- HIPAA requires the protection and confidential handling of *protected health information* (PHI) in all forms (verbal, written, electronic).
- HIPAA Rules apply to *covered entities*
  - hospitals, dental clinics, other facilities that bill Medicaid
  - employees who work in/for these facilities
  - *HIPAA does not cover FERPA-regulated entities/employees*

Protected Health Information

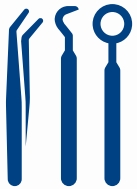
- Protected health information (PHI) – any health-related information that can be used alone, or in combination with other info., to identify an individual.
  - Names of individuals and relatives
  - Mailing and E-mail addresses
  - Health plan beneficiary numbers

HIPAA

- PHI can only be used and disclosed – to the *minimum necessary* – for specific purposes:
  - Treatment
  - Payment
  - Healthcare operations
- *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



HIPAA Scenarios



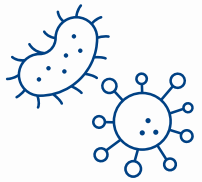
- A school dental sealant provider gave report to their DCO or FQHC, including patient assessment details.

- A clinic case manager sent patient information to the dental billing office, including patient insurance plan numbers and diagnostic codes.
- A care facility trained employees on preventing medication errors. The training included information about number of errors that occurred each month in the past year, without naming the patients involved.

Oregon Health Authority

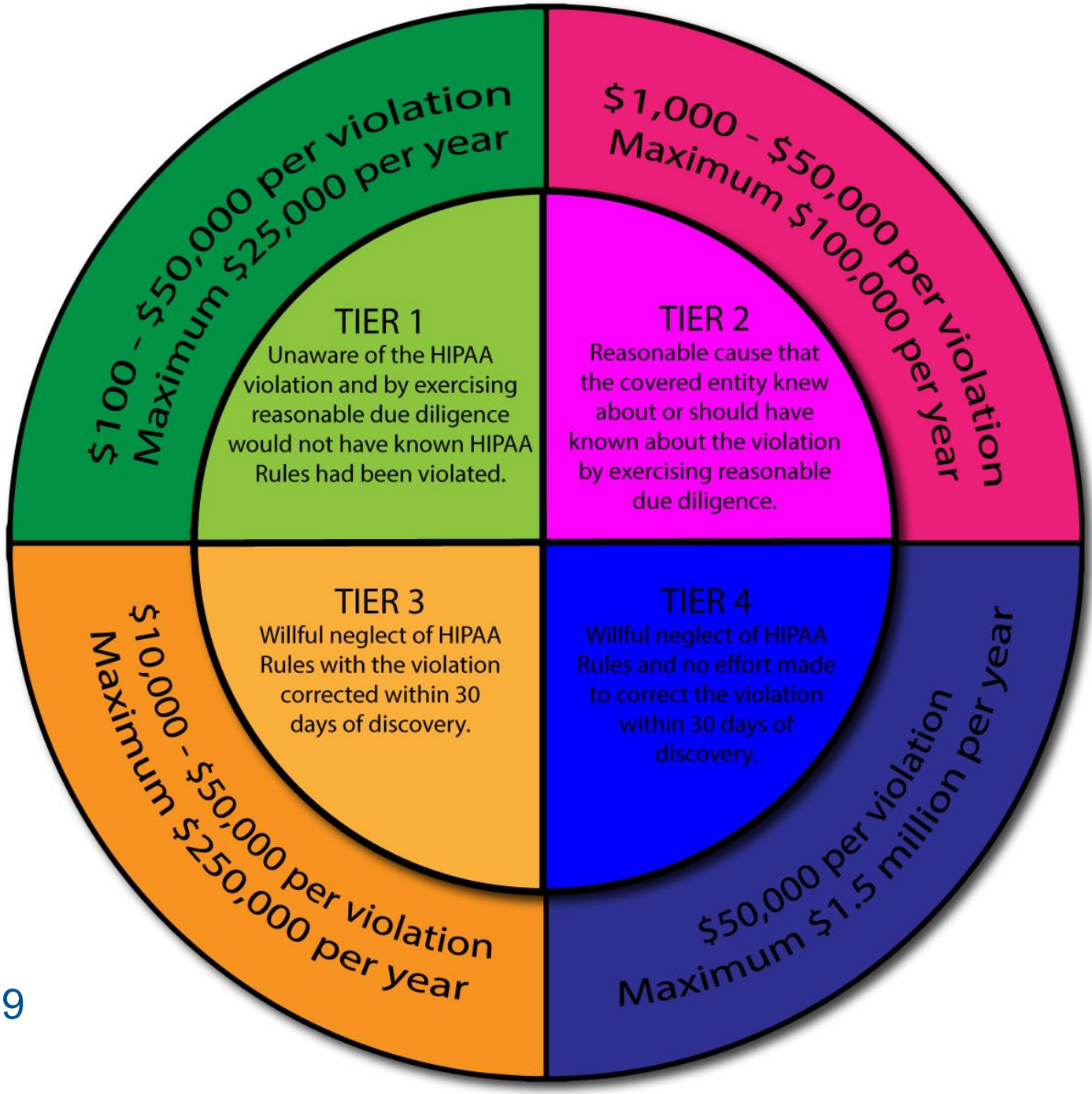
HIPAA Rule During Emergencies

- It is permissible to share PHI with public health authorities such as the CDC, state and local public health authorities, and others responsible for ensuring the safety of the public.
- In such cases PHI may be shared without obtaining authorization from the patient.



Oregon Health Authority

HIPAA Violations



HIPAA Journal 2019

HIPAA questions

Oregon Health Authority

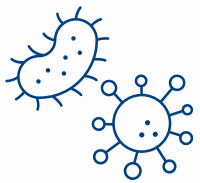
FERPA Regulations

- FERPA protects the privacy of *student education records* which are 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 (student ID number, social security number)
  - Grades, academic transcript
  - Attendance record
  - School health records

Oregon Health Authority

FERPA Regulations

- Parents/guardians may access their minor student's entire educational record.
- School staff who have *legitimate educational interest* may be granted access to specific information, without prior consent.
- Directory information may be disclosed without prior consent if the school has adopted policies, and parents have not opted out of disclosure
- Public health emergencies – PHI may be disclosed to public health authorities without prior consent, when necessary for public health and safety



Oregon Health Authority

FERPA questions

Oregon Health Authority

Could this be a privacy violation?

Student: “Why did my friend get a happy face on their paper and I got a sad face?”

Oregon Health Authority

Preventing a privacy violation

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.

Could this be a privacy violation?

School administrator: “I’ll need the list of which students were screened today.”

Preventing a privacy violation

- Permission form (Consent form / Release of information / Privacy Policy) may clarify
- *Minimum necessary* per HIPAA
  - Clinic / dental provider: treatment record per protocol
  - Student / family: treatment record (full details)
  - School staff: screening/sealants were completed; recommendation to follow up (ODE reporting does not require details; Permission form may allow additional sharing for care coordination)
- Consider how to share *minimum necessary* while keeping information secure

Oregon Health Authority

Examples of Security Incidents

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

Privacy and 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

Could this be a privacy violation?

Parent: “Thanks for letting me into the treatment space. I see my neighbor’s kid getting treated. Can I get a copy of the notes? I’ll drop them off this afternoon.”

Oregon Health Authority

Preventing a privacy violation

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.

- Prevent unauthorized entry and report any “tailgating” incidents to the front office right away.

Access Controls

- Never let anyone – even someone you recognize – follow you into a secured area (including schools).
- 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.

Privacy & Security In Practice

- Client-level data, either in paper or electronic format, should be secured at all times:
  - Hide completed forms from sight or take the iPad/laptop with you during breaks and at lunchtime.
  - Store completed forms and technology in secure locations at home or in a hotel room safe *(not visible in a car)*
  - Use tamper resistant envelopes.
  - When in transit to a school or home, securely lock completed forms or an iPad/laptop in a vehicle trunk or hidden from sight.

Special considerations

- Consent forms, release of information
- School protocols for COVID-19

Privacy & Security In Practice

- Distribute HIPAA forms (i.e. notice of privacy practices) along with parent/guardian permission forms.
  - Opt-out notices are also used in some settings, generally with MOU in place
  - Be familiar with approved information sharing per privacy practices and permission forms

Privacy & Security In Practice

COVID-19 considerations

- Verify guidance for dental sealants programs and site-specific district/school protocols

  - *Collect required client-level data*
    - Add special fields as needed (i.e. temperature reading)
    - Track visits; who was present (LPHA reporting/notifications if there is a positive case)

  - *Maintain or increase infection control measures*
    - procedures for disinfecting computers, laptops, iPads, etc.
    - PPE per employer and facility protocols (may include face covering for students waiting in treatment space)

Questions

Oregon Health Authority