HIPAA COMPLIANCE FOR DENTAL PROFESSIONALS

Mary Govoni, MBA, RDH, CDA

1

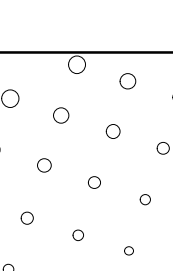
LEARNING OBJECTIVES

- 1 – Discuss the purpose of HIPAA and its history.
- 2 – Identify HIPAA compliance requirements for dentistry.
- 3 – Develop strategies for protecting PHI.
- 4 – Identify privacy and security risks to PHI.

2

THE WHAT AND WHY OF HIPAA RULES

3



What is HIPAA?

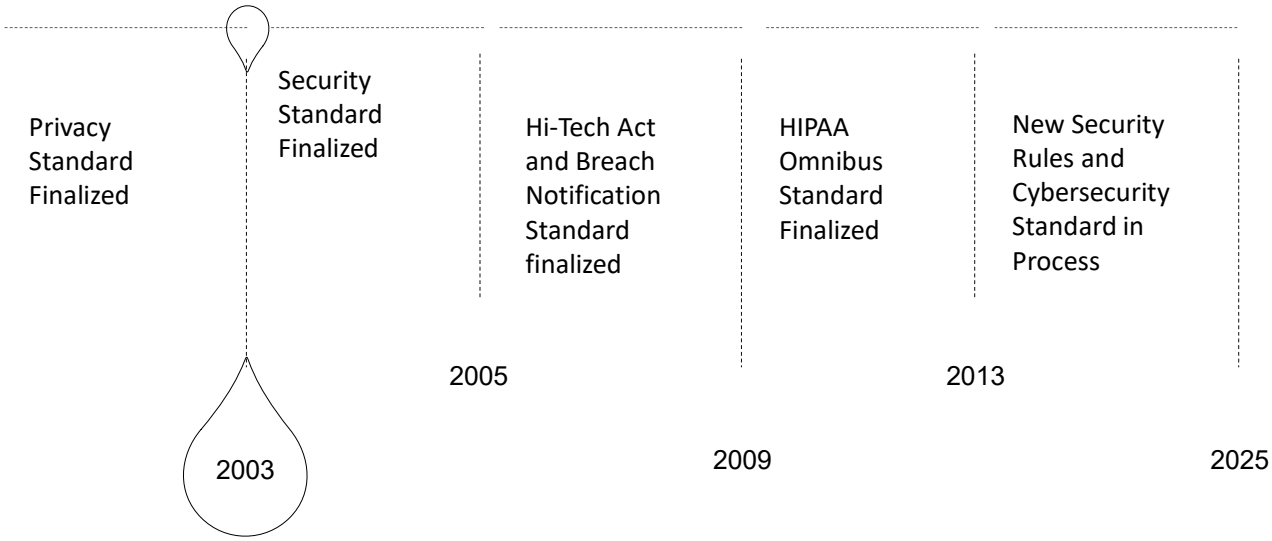
Health Insurance Portability and Accountability Act

- Provides protections for patients' health care information
- Requires Covered Entities to safeguard the privacy and security of electronic patient data

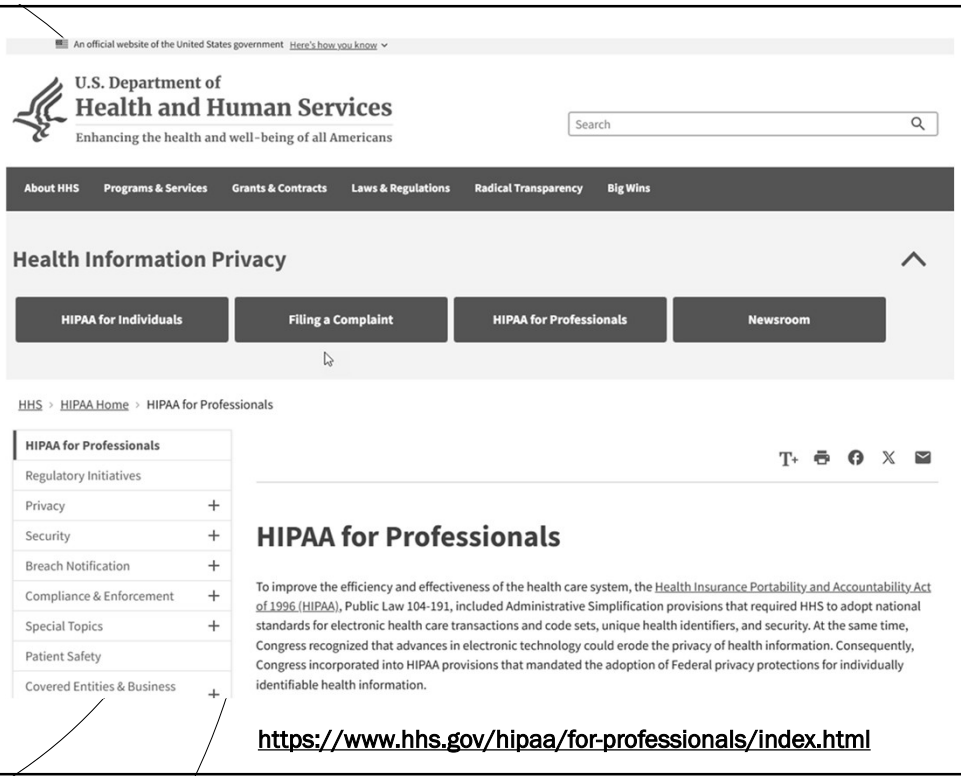
Puts in place specific requirements for protection against cybersecurity attacks that access or steal patients' data

4

HIPAA Timeline



5



6

POTENTIAL UPDATES TO HIPAA SECURITY RULES AND CYBERSECURITY RULE

- New HIPAA security rule passed in 2024
  - Currently under review
    - https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/index.html
- New Cybersecurity Rule – HISAA
  - Health Infrastructure Security and Accountability Act
    - https://www.healthlawadvisor.com/hisaa-new-federal-legislation-introduced-that-would-create-significant-new-cybersecurity-requirements-for-hipaa-covered-entities-and-business-associates
- If implemented will have major changes in requirements for dental practices/facilities.

7

PROTECTED HEALTH INFORMATION (PHI)

- Personal information
  - name, address, phone no., soc. sec. no., etc.
- Dental and medical history and tx
- All other info in patient chart/EHR

8

PROTECTED HEALTH INFORMATION (PHI)

How PHI is used:

- Treatment, Payment and Health Care Operations - TPO
  - Referral to a specialist
  - Submission of claims for payment
  - Sending account to collections
- Non-TPO
  - Selling or disclosing patient mailing list to a company for marketing purposes
  - Presentations – study clubs, seminars, etc.

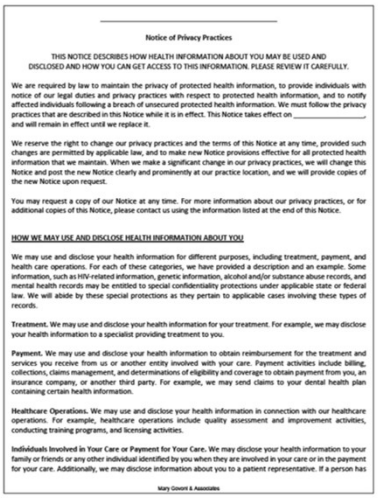
9

HIPAA-REQUIRED DOCUMENTATION

10

HIPAA-REQUIRED DOCUMENTS

- Training records
- Business associate agreements (BAA)
- Privacy and security policies
- Notice of privacy practices (NPP)
- HIPAA acknowledgement form from patients
  - Document which individuals with whom tx may be discussed
- Records of any patient complaints or employee incidents
  - Violation of privacy or security rules



Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW HEALTH INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

We are required by law to maintain the privacy of protected health information, to provide individuals with notice of our legal duties and privacy practices with respect to protected health information, and to notify affected individuals following a breach of unsecured protected health information. We must follow the privacy practices that are described in this Notice while it is in effect. This Notice takes effect on _____, and will remain in effect until we replace it.

We reserve the right to change our privacy practices and the terms of this Notice at any time, provided such changes are permitted by applicable law, and to make new Notice provisions effective for all protected health information that we maintain. When we make a significant change in our privacy practices, we will change this Notice and post the new Notice clearly and prominently at our practice location, and we will provide copies of the new Notice upon request.

You may request a copy of our Notice at any time. For more information about our privacy practices, or for additional copies of this Notice, please contact us using the information listed at the end of this Notice.

HOW WE MAY USE AND DISCLOSE HEALTH INFORMATION ABOUT YOU

We may use and disclose your health information for different purposes, including treatment, payment, and health care operations. For each of these categories, we have provided a description and an example. Some information, such as HIV-related information, genetic information, alcohol and/or substance abuse records, and mental health records may be entitled to special confidentiality protections under applicable state or federal law. We will abide by these special protections as they pertain to applicable cases involving these types of records.

Treatment. We may use and disclose your health information for your treatment. For example, we may disclose your health information to a specialist providing treatment to you.

Payment. We may use and disclose your health information to obtain reimbursement for the treatment and services you receive from us or another entity involved with your care. Payment activities include billing, collections, claims management, and determinations of eligibility and coverage to obtain payment from you, an insurance company, or another third party. For example, we may send claims to your dental health plan containing certain health information.

Healthcare Operations. We may use and disclose your health information in connection with our healthcare operations. For example, healthcare operations include quality assessment and improvement activities, conducting training programs, and licensing activities.

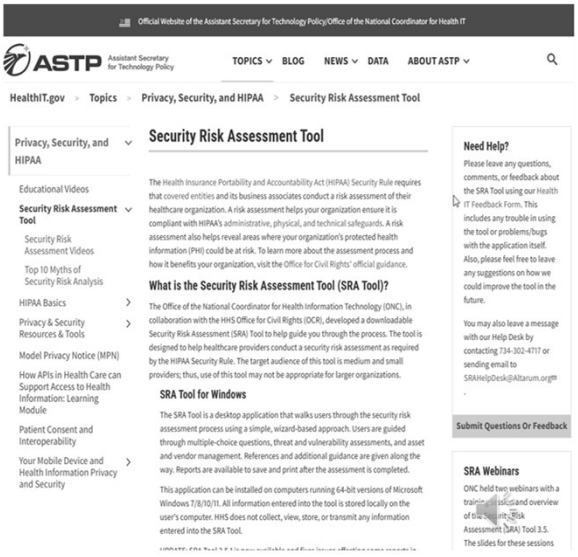
Individuals Involved in Your Care or Payment for Your Care. We may disclose your health information to your family or friends or any other individual identified by you when they are involved in your care or in the payment for your care. Additionally, we may disclose information about you to a patient representative. If a person has

Mary Govoni & Associates

11

HIPAA-REQUIRED DOCUMENTS

- Annual security risk assessment
  - https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html
  - https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool
- Assessment of any security breaches
- Notifications to patients of a security breach
- Notifications to the Dept. of HHS of a security breach
- A contingency plan for emergency operations in case of a breach or disaster situation



Official Website of the Assistant Secretary for Technology Policy/Office of the National Coordinator for Health IT

ASTP Assistant Secretary for Technology Policy

TOPICS BLOG NEWS DATA ABOUT ASTP

HealthIT.gov > Topics > Privacy, Security, and HIPAA > Security Risk Assessment Tool

Privacy, Security, and HIPAA

Educational Videos

Security Risk Assessment Tool

Security Risk Assessment Videos

Top 10 Myths of Security Risk Analysis

HIPAA Basics

Privacy & Security Resources & Tools

Model Privacy Notice (MPN)

How APIs in Health Care can Support Access to Health Information: Learning Module

Patient Consent and Interoperability

Your Mobile Device and Health Information Privacy and Security

Security Risk Assessment Tool

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that covered entities and its business associates conduct a risk assessment of their healthcare organization. A risk assessment helps your organization ensure it is compliant with HIPAA's administrative, physical, and technical safeguards. A risk assessment also helps reveal areas where your organization's protected health information (PHI) could be at risk. To learn more about the assessment process and how it benefits your organization, visit the Office for Civil Rights' official guidance.

What is the Security Risk Assessment Tool (SRA Tool)?

The Office of the National Coordinator for Health Information Technology (ONC), in collaboration with the HHS Office for Civil Rights (OCR), developed a downloadable Security Risk Assessment (SRA) Tool to help guide you through the process. The tool is designed to help healthcare providers conduct a security risk assessment as required by the HIPAA Security Rule. The target audience of this tool is medium and small providers; thus, use of this tool may not be appropriate for larger organizations.

SRA Tool for Windows

The SRA Tool is a desktop application that walks users through the security risk assessment process using a simple, wizard-based approach. Users are guided through multiple-choice questions, threat and vulnerability assessments, and asset and vendor management. References and additional guidance are given along the way. Reports are available to save and print after the assessment is completed.

This application can be installed on computers running 64-bit versions of Microsoft Windows 7/8/10/11. All information entered into the tool is stored locally on the user's computer. HHS does not collect, view, store, or transmit any information entered into the SRA Tool.

Need Help?

Please leave any questions, comments, or feedback about the SRA Tool using our Health IT Feedback Form. This includes any trouble in using the tool or problems/bugs with the application itself. Also, please feel free to leave any suggestions on how we could improve the tool in the future.

You may also leave a message with our Help Desk by contacting 734-302-4717 or sending email to SRAHelpDesk@Altarum.org.

Submit Questions Or Feedback

SRA Webinars

ONC held two webinars with a training session and overview of the Security Risk Assessment (SRA) Tool 3.5. The slides for these sessions

12

BUSINESS ASSOCIATE AGREEMENTS

13

BAAs

Agreements/contracts with individuals and business who require access to PHI

- Includes any subcontractors

Tech companies and services frequently have their own agreements

- Dental covered entity must ascertain that the company is HIPAA compliant

Cleaning service contractors not covered

- Need a confidentiality agreement

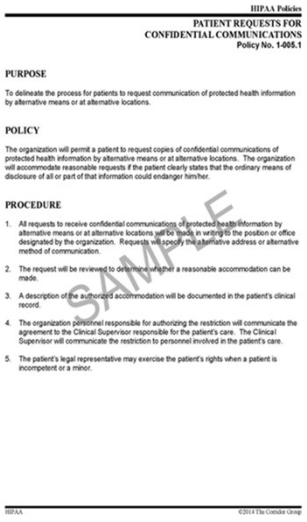
14

PRIVACY AND SECURITY POLICIES AND DOCUMENTATION

15

PRACTICE-SPECIFIC POLICIES

- Privacy and Security Policies
- Notice of Privacy Practices
- Patient Acknowledgement form
- Templates available from DHHS and purchased manuals
  - Must be reflect the practice's protocols.
  - Don't just fill in the blanks on a template – must be customized.
  - Policies must be updated annually.



HIPAA Policies

PATIENT REQUESTS FOR CONFIDENTIAL COMMUNICATIONS
Policy No. 1-005.1

PURPOSE

To delineate the process for patients to request communication of protected health information by alternative means or at alternative locations.

POLICY

The organization will permit a patient to request copies of confidential communications of protected health information by alternative means or at alternative locations. The organization will accommodate reasonable requests if the patient clearly states that the ordinary means of disclosure of all or part of that information could endanger him/her.

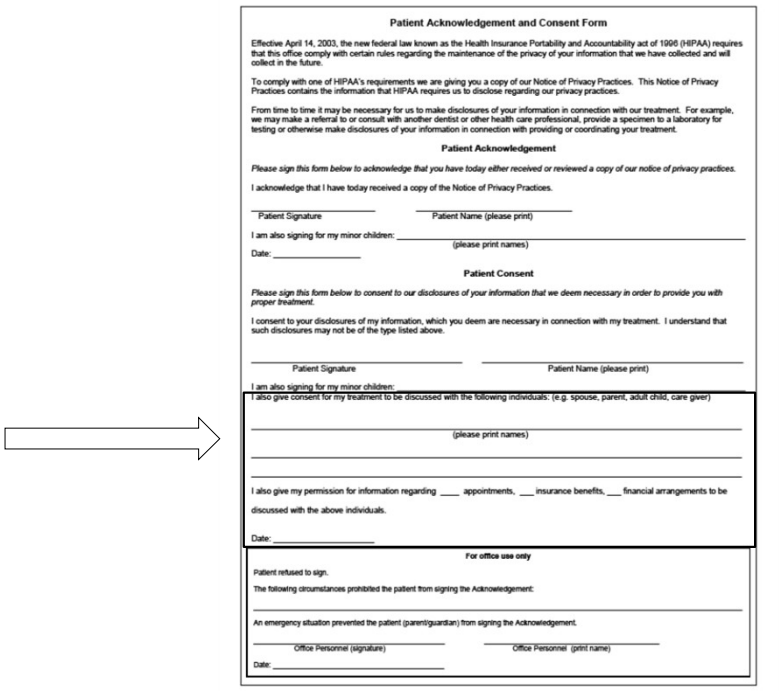
PROCEDURE

1. All requests to receive confidential communications of protected health information by alternative means or at alternative locations will be made in writing to the position or office designated by the organization. Requests will specify the alternative address or alternative method of communication.
2. The request will be reviewed to determine whether a reasonable accommodation can be made.
3. A description of the authorized accommodation will be documented in the patient's clinical record.
4. The organization personnel responsible for authorizing the restriction will communicate the agreement to the Clinical Supervisor responsible for the patient's care. The Clinical Supervisor will communicate the restriction to personnel involved in the patient's care.
5. The patient's legal representative may exercise the patient's rights when a patient is incompetent or a minor.

SAMPLE

HIPAA ©2014 The Consilio Group

16



Patient Acknowledgement and Consent Form

Effective April 14, 2003, the new federal law known as the Health Insurance Portability and Accountability act of 1996 (HIPAA) requires that this office comply with certain rules regarding the maintenance of the privacy of your information that we have collected and will collect in the future.

To comply with one of HIPAA's requirements we are giving you a copy of our Notice of Privacy Practices. This Notice of Privacy Practices contains the information that HIPAA requires us to disclose regarding our privacy practices.

From time to time it may be necessary for us to make disclosures of your information in connection with our treatment. For example, we may make a referral to or consult with another dentist or other health care professional, provide a specimen to a laboratory for testing or otherwise make disclosures of your information in connection with providing or coordinating your treatment.

Patient Acknowledgement

Please sign this form below to acknowledge that you have today either received or reviewed a copy of our notice of privacy practices.

I acknowledge that I have today received a copy of the Notice of Privacy Practices.

Patient Signature _____ Patient Name (please print) _____

I am also signing for my minor children: _____ (please print names)

Date: _____

Patient Consent

Please sign this form below to consent to our disclosures of your information that we deem necessary in order to provide you with proper treatment.

I consent to your disclosures of my information, which you deem are necessary in connection with my treatment. I understand that such disclosures may not be of the type listed above.

Patient Signature _____ Patient Name (please print) _____

I am also signing for my minor children:

I also give consent for my treatment to be discussed with the following individuals: (e.g. spouse, parent, adult child, care giver)

_____ (please print names)

_____

_____

I also give my permission for information regarding ____ appointments, ___ insurance benefits, ___ financial arrangements to be discussed with the above individuals.

Date: _____

For office use only

Patient refused to sign.

The following circumstances prohibited the patient from signing the Acknowledgement:

_____

An emergency situation prevented the patient (parent/guardian) from signing the Acknowledgement.

Office Personnel (signature) _____ Office Personnel (print name) _____

Date: _____

17

APPLICATION OF HIPAA PRIVACY RULES

- **Designate a Privacy Officer/Manager**
  - Oversees compliance
  - Addresses incidents and complaints
- **Get written permission to talk to others about patient treatment**
  - Not necessary for parents/guardians of minor children
- **Conversations with patients/parents of patients**
  - Do not discuss treatment in reception area when others are present.
- **Obtain permission to leave voicemail messages.**
  - Ask patients how they want you to communicate with them
- **Use a HIPAA-compliant app for texting and confirming appointments.**

18

APPLICATION OF HIPAA PRIVACY RULES

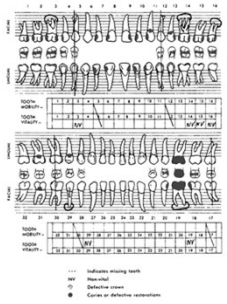
- Never send PHI (radiographs, etc.) through unencrypted email.
- Do not leave patient charts unsecured when leaving the office for the night when cleaners come into the office.
  - Lock up paper charts
  - Log off all computer workstations

This Photo by Unknown Author is licensed under CC BY

- Verify the identity of patients, parents/guardians
  - Photo ID – driver's license or gov't issued ID
- Verify identity of person to whom you are disclosing information
  - On phone – ask for DOB

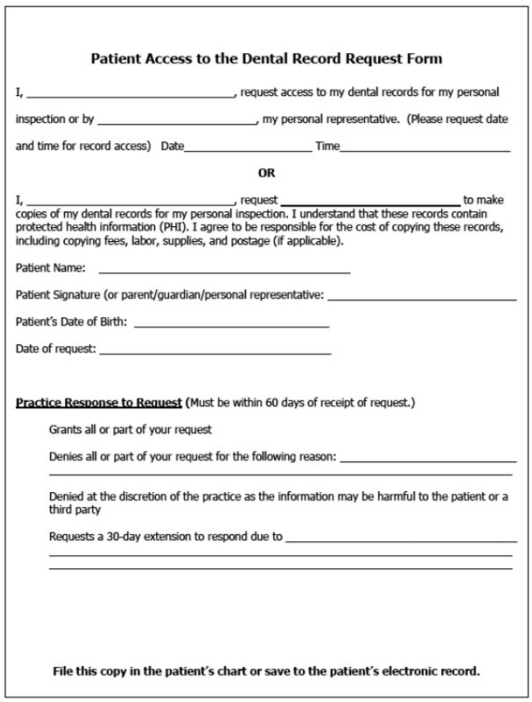
19

PATIENT'S RIGHTS UNDER HIPAA



- Patient's have the right to:
  - Access or obtain a copy of their records
  - Practices have 15 days to comply
  - Patient's must make the request in writing
  - Access to or copies of records CANNOT be withheld until an account balance is paid in full.

20



Patient Access to the Dental Record Request Form

I, _____, request access to my dental records for my personal inspection or by _____, my personal representative. (Please request date and time for record access) Date_____ Time_____

OR

I, _____, request _____ to make copies of my dental records for my personal inspection. I understand that these records contain protected health information (PHI). I agree to be responsible for the cost of copying these records, including copying fees, labor, supplies, and postage (if applicable).

Patient Name: _____

Patient Signature (or parent/guardian/personal representative: _____

Patient's Date of Birth: _____

Date of request: _____

Practice Response to Request (Must be within 60 days of receipt of request.)

Grants all or part of your request

Denies all or part of your request for the following reason: _____

Denied at the discretion of the practice as the information may be harmful to the patient or a third party

Requests a 30-day extension to respond due to _____

File this copy in the patient's chart or save to the patient's electronic record.

21

TRANSFER OF PATIENT RECORDS

- CEs must account for all disclosures of patient PHI
  - Referrals to other dental or medical professionals are covered by TPO
    - Enter referral and transfer into clinical notes
  - If patient is transferring to a new practice, they must sign a form giving permission to transfer to a specific provider.
  - If a new patient is transferring to the practice, the patient's previous provider must have a copy of a signed request for transfer.

Permission to Transfer Dental Records

Patient information:

Name: _____

Address: _____

_____

Phone: _____

(home, cell, work)

New Dentist/Dental Practice Information to Transfer Records:

Name: _____

Address: _____

_____

Phone: _____

Email: _____

I give permission to transfer and request that my dental x-rays and/or other diagnostic images be transferred to the above named dental/dental practice.

Name of patient's personal representative (if applicable) _____

Name of parent or guardian (if patient is a minor) _____

_____ _____

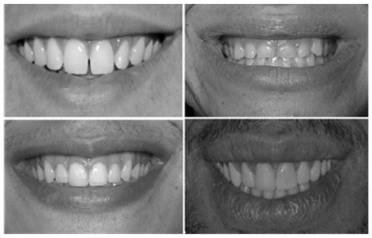
Signature of patient, personal representative or guardian Date

Please note that x-rays cannot be transferred without the patient's signature or the signature of the patient's personal representative or parent/guardian, if the patient is a minor. Copies of x-rays and other diagnostic images will be sent. All original x-rays and images are the property of this practice. This practice sends email with patient information through an encryption portal and will not send information through an unsecure email network.

22

USE OF PATIENT IMAGES

- CEs must obtain written permission to use patient images for use by the provider or practice in/on:
  - Social media
  - Presentations
    - Seminars/study clubs
    - Consultations
  - Before and after photo displays



- Patients can request an accounting for how those images were used.
- Patients must also sign a model release
  - To avoid having to pay royalties

23

Authorization Form for Release of Protected Health Information
For Non-Treatment, Payment or Operations (TPO)

Patient Name_____ Patient's Date of Birth_____

I hereby authorize the use and disclosure of individually identifiable dental health information relating to me as described below. I understand that information disclosed pursuant to this authorization may be subject to re-disclosure by the recipient and may no longer be protected by HIPAA Privacy regulations.

Specific Description of Information to Be Used or Disclosed:

Purpose for Disclosure: _____

I authorize the following person(s) to make the requested use or disclosure of the above health information.

Person(s) Receiving My Authorized Information Include_____

I understand that I may revoke this authorization at any time by notifying _____ in writing. If I choose to do so, my revocation will not affect any actions taken by _____ before receiving my revocation.

I understand that I may refuse to sign this authorization; and that my refusal to sign in no way affects my treatment, payment, enrollment in a health plan, or eligibility for benefits.

This Authorization Expires on _____

Signature of Patient or Patient's Personal Representative

_____Date_____

If Personal Representative
Print Name_____
Signature _____Relationship to Patient_____

For office use only: Copy of signed authorization provided to the individual: Date:_____ Initials____.

File this form in the patient's chart or electronic record.

Mary Govoni & Associates

Model Release Agreement

I _____, hereby grant _____ the unrestricted right to use, reproduce, and publish photographs of me taken on _____ (date), for any lawful purpose, including, but not limited to marketing, trade, or any other commercial or artistic medium, known or later developed.

I represent and warrant that I am at least 18 years of age, and have full legal capacity to execute this agreement for myself or my minor child. I have ready and fully understand the contents of this release.

I acknowledge that _____ owns the copyright on these photographs and I hereby waive any claims that I may have on any usage of the photographs, or works derived thereof, including but not limited to claims for invasion of privacy, publicity, or defamation.

I agree that I will receive no compensation for this release and all rights granted hereunder.

Name of Model: _____ Witness Name: _____

Model's Date of Birth Witness Signature

Signature of Model: _____

Date: _____

24

HIPAA, CYBERSECURITY AND THE PREVENTION OF SECURITY BREACHES

25

How do security breaches happen?

- **Insider threats – employees, visitors, vendors in the practice**
  - Inappropriate us of internet by employees
  - Unauthorized access
- **Hackers**
  - Break through firewall and security software
  - Steal PHI for financial gain
- **Email that is infected with malware/ransomware/viruses**
- **Theft**

26

Signs of an Intrusion or Breach

- Problems starting up computer
- Files cannot be accessed
- Unexpected pop-up windows
- Message that states files are locked

27

Key Strategies for Cybersecurity

- Train the team.
- Document security policies.
- Enforce internet use policy.
- Protect your data (passwords, PMS software, security software/hardware).
- Back up your data and verify back-ups.
- Hire and IT professional who specializes in healthcare settings.

Take-Aways

28

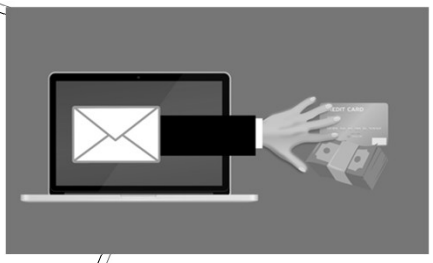
TEAM TRAINING FOR CYBERSECURITY

- What is the practice internet protocol – and why?
  - NO use of workstations for personal business
  - NO downloading of games, music, menus, etc.
- What are the risks of using the office "intranet"?
  - Breaches
  - Malware
- How is the patient data and server protected?
  - Software and monitoring
  - Hardware - firewalls
- What are some signs of a potential security breach?
- What is the practice protocol for email security?

29

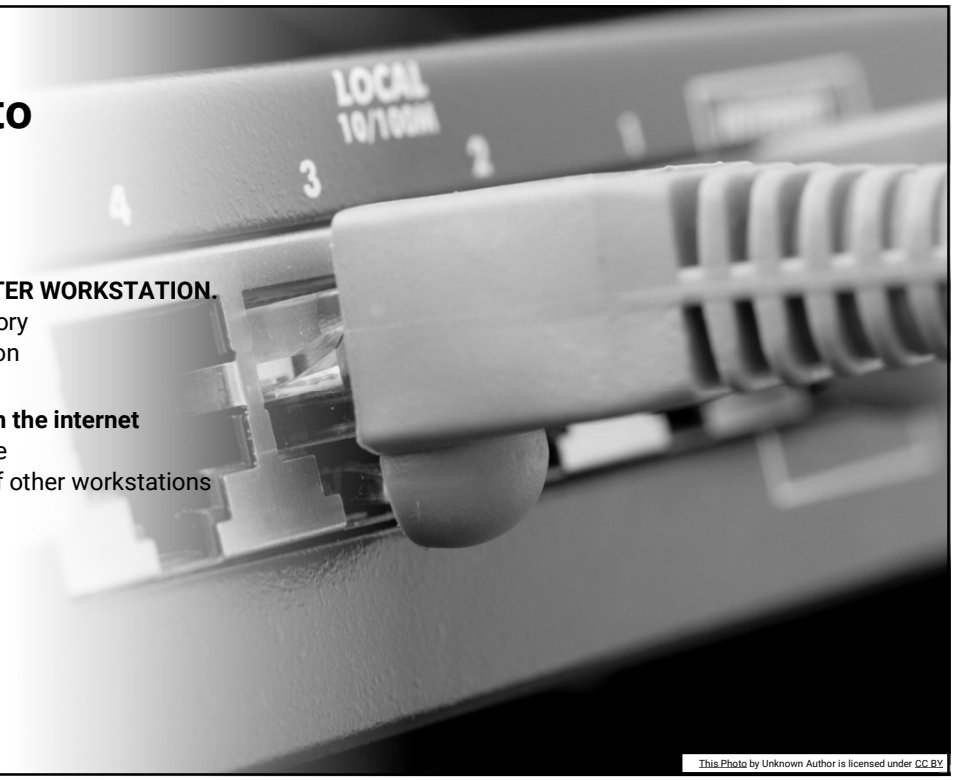
Email Breaches

- Do not use free email – it is not secure.
  - Gmail, Yahoo, etc.
- Use secure email for all communications.
  - Use email based on your web URL e.g. info@mydentalpractice.com
- Use encryption or VPN for sending patient information



30

Initial Response to a Suspected Breach



- **DO NOT TURN OFF COMPUTER WORKSTATION.**
  - May delete browsing history
  - Necessary for investigation
- **Disconnect workstation from the internet**
  - Pull out the ethernet cable
  - Helps prevent infection of other workstations
- **Call IT support immediately**
  - Follow their instructions

31

Preventing Breaches

- Follow all privacy and security policies and protocols for the practice.
- Provide training to all employees – new and continuing.
- Work with an IT professional to implement safeguards as required by DHHS/HIPAA rules.

32

THANK YOU!

Mary Govoni, MBA, RDH, CDA
mary@marygovoni.com
www.marygovoni.com
517.214.8223

33