Emailing Patient Information: A Resource for Dental Practices

Dental practices may have questions about how to use email and whether they should encrypt emails that contain any patient information. HIPAA doesn't prohibit emailing patient information in an unencrypted form, although in order to do so covered dental practices must:

- Do a written ***risk assessment***
- Have ***reasonable safeguards***
- Send ***breach notification*** if patient information is compromised
- Honor certain ***patient requests*** for unencrypted email

The ***risk assessment*** must take into account all of the dental practice's electronic patient information, such as electronic dental records, digital radiographs, and email. The dental practice must assess where the information is vulnerable, the threats to the information, and the likelihood and severity of the risk of compromise. The dental practice must also document how it complies with the HIPAA security standards and specs.

Examples of ***reasonable safeguards*** may include checking the e-mail address for accuracy before sending, or limiting the amount or type of information that may be sent in an unencrypted e-mail.

If patient information is compromised, a dental practice must send ***breach notification***. For example, if a dental practice sent an email containing unencrypted information about a patient to the wrong email address, the dental practice would likely have to notify the patient of the breach, and include information about the incident in the breach log that it submits annually to the federal Office for Civil Rights. Information about HIPAA breach notification is available on the ADA website and the Office for Civil Rights website.

HIPAA may require a dental practice to honor a ***patient request*** to send his or her patient information via email if, for example, if a patient asks the dental practice to communicate with him or her via email and the practice determines that the request is reasonable, or if a patient asks the dental practice to send his or her electronic dental or payment records in an unencrypted email, and still insists after the dental practice has warned of the risk. Similarly, HIPAA may require a dental practice NOT to send the information via email if a patient so requests.

To help dental practices better understand these HIPAA requirements, the ADA has developed the sample documents in this resource. The sample forms in this resource include:

- A risk assessment for emailing patient information
- Policies and procedures that state the safeguards the dental team must use when emailing patient information
- An authorization form for a patient to use to consent to unencrypted email **(must be a stand-alone document)**
- A Notice of Privacy Practices with a section on email

These documents only illustrate one way that a dental practice might approach email. Every dental practice is different, and each practice must make decisions about email based on its own risk assessment. For example, some practices might decide to use a secure email service some or all of the time. Other practices might decide not to use email at all, unless HIPAA requires them to do so

PLEASE NOTE that:

(1) These sample forms apply to email ONLY and do not illustrate the complete Risk Assessment as required by HIPAA's Security Rule.

(2) ***Every office must conduct its own risk assessment and make changes to these sample forms as applicable in compliance with HIPAA.***

The ADA is grateful for the assistance of the New Jersey Dental Association in the development of this member resource.

Sample HIPAA Security Risk Assessment for a Small Dental Office
Emailing Unsecured Patient Information

Date: _____

What are the potential vulnerabilities?

Emails from our dental practice may contain ePHI, and our emails are not encrypted in a way that makes them "secure" under the HIPAA Breach Notification Rule.

What are the potential threats?

Unauthorized individuals might access unsecured ePHI in transit. ePHI may be accessed by unauthorized individuals if an unsecured email is sent to the wrong email address, or if an email has the wrong attachment. If our dental practice discovers a breach of unsecured PHI, we must provide notification in compliance with the HIPAA Breach Notification Rule.

Is the risk low, medium or high in light of (1) the likelihood that it will happen, and (2) the potential severity?

The threat is low in terms of both likelihood and severity. [***NOTE: The threat is likely low if the following statements are true. Each practice should perform its own risk assessment of its current practices.***]

(1) Our dental practice rarely, if ever, emails ePHI. When we do, we generally do so only to: send an appointment reminder; respond to a question emailed by a patient; or send radiographs to another doctor's office. The ePHI contained in those messages generally includes only the patient's name, demographic information and/or dental x-ray. We have a policy in place against emailing sensitive information such as Social Security numbers, credit and debit card numbers, drivers' license numbers, or sensitive health information such as mental health information, genetic information, substance abuse/alcoholism, or positive infection status (e.g., HIV). We only send such sensitive information in an unencrypted email if the patient insists after we have warned the patient of the risk. In addition, we do not send emails containing the PHI of more than one individual at a time. We are not aware of any email being accessed by an unauthorized individual, sent to the wrong email address, or sent with the wrong attachment.

(2) If an unauthorized individual accessed a typical email from our office, it is unlikely that any harm would result to the patient. Our dental practice understands that in such an instance, it would need to provide notification if required by the HIPAA Breach Notification Rule and/or applicable state law.

The HIPAA standard titled "Transmission Security" requires our dental practice to "address" the following specs:

1. Integrity controls:

   Would the following be a reasonable and appropriate safeguard in our dental practice environment (that is, would it be reasonable to adopt the following to help protect ePHI given the size of our practice and the likelihood of the risk)?: *security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.*

   *Yes __ No _X_*

   Explain why or why not:

   Except for dental images, appointment reminders and demographic information, our dental practice emails medical record information only in .PDF form, thus assuring the information may not be modified in any way. Adding additional security measures to assure that other ePHI is not modified is not reasonable or appropriate for our dental practice. The only way our dental practice transmits ePHI is via email. Our practice uses email to transmit ePHI only infrequently (e.g., approximately ___ per month) and our existing email system does not feature additional integrity controls. Adding additional integrity controls would be unreasonably expensive for our dental practice. As the ePHI emailed generally includes only demographic information, appointment dates and dental x-rays, our dental practice believes it is unlikely that an email would be improperly modified, and the resulting impact is not likely to be material. E.g., if a patient receives an appointment reminder with the wrong

date, or if a dental specialist receives an unreadable x-ray, in each case the recipient is likely to contact the practice to obtain a revised copy of the information received.

Is there an equivalent alternative?
If someone notifies us that an email appears to have been modified, we will resend the email or provide the information by another means.

2. Encryption

Would the following be a reasonable and appropriate safeguard in our dental practice environment (that is, be reasonable to adopt the following to help protect ePHI given the size of our practice and the likelihood of the risk)?: *a mechanism to encrypt ePHI in transit whenever deemed appropriate.*

Yes ___ No __X__

Explain why or why not:

Such a mechanism would not be reasonable and appropriate for our dental practice. Our dental practice does not routinely email ePHI, and when we do we never include information that is sensitive in nature unless the patient insists after we have warned the patient of the risk. A mechanism to encrypt ePHI would be unreasonably expensive for our dental practice. Our dental practice believes it is unlikely that an unencrypted email would be accessed by an unauthorized individual, and the resulting impact would not likely be severe, because the ePHI our dental practice sends via email generally contains only appointment reminders and/or dental x-rays.

Is there an equivalent alternative?

Our dental practice will:

- Notify individuals in our Notice of Privacy Practices that we do not encrypt emailed ePHI
- Prior to using email as a permissible form of communication with respect to our patients' ePHI, ask individuals to sign a HIPAA-compliant authorization permitting our dental practice to email unencrypted ePHI to the individuals or others as may be necessary from time to time
- Send PHI of patients who do not consent via other means, which may include asking the patient to hand deliver the PHI
- Train staff:
    - to double check email addresses for accuracy before sending an email
    - where appropriate, to send an email for address confirmation prior to emailing PHI (for example, if the email address is handwritten and the handwriting is hard to read)
    - unless the patient has otherwise authorized the practice to do so, to exclude sensitive information from the type of information sent via email
    - if a patient asks our dental practice not to email him or her, to accommodate this request
- If a patient emails our dental practice, assume that email communications are acceptable to the patient. Even so, our dental practice will use good faith efforts to confirm with the individual that emailing of unencrypted ePHI is permissible as set forth above.

Email Policies and Procedures Effective _____, 20___

1. We do not have a secure email service and we cannot encrypt emails. We generally do not email patient information. When we do, we typically only send:
    a. Appointment reminders to patients
    b. Responses to questions emailed by patients
    c. Radiographs to another doctor's office

2. Our emails should generally include only the patient's name, demographic information (for example, name and address), and/or radiographs.

3. Check the email address for accuracy before sending an email. Where appropriate, send an email for address confirmation prior to emailing PHI (for example, where the email address is handwritten and the handwriting is hard to read).

4. Do not send email to a patient who has asked our dental practice not to email him or her.

5. If a patient emails our dental practice, we can assume that email communications are acceptable to the patient. Even so, if possible, ask the patient to sign our Email Authorization Form before sending an email.

6. Do not email sensitive information such as Social Security numbers, credit and debit card numbers, drivers' license numbers, mental health information, genetic information, substance abuse/alcoholism, or positive infection status (e.g., HIV) unless the patient insists.

7. Do not email patient information unless the patient has signed our Email Authorization Form. Give the patient a copy of the signed form.

8. If a patient refuses to sign our Email Authorization Form, ask the patient to deliver any sensitive patient information, or send it via some other means, such as U.S. Mail or regular (non-digital) fax.

9. Do not send emails containing information about more than one patient.

10. Always use a .PDF format when sending patient information (except for appointment reminders, radiographs, or demographic information like name and address). This is because PDFs cannot be modified in transit.

11. If someone notifies us that an email appears to have been modified (for example, if a radiograph is unreadable), we will resend the email or provide the information by some other means.

12. IMMEDIATELY report to the Privacy Official if you discover that patient information has been sent to or accessed by anyone other than the patient or intended recipient.

Authorization and Consent
To Send Unencrypted Patient Information by Email and Other Electronic Means

Until I tell you in writing to stop, I authorize <**Dental Practice**> to transmit patient information relating to my treatment, health, or payment by email or other electronic means, without encryption or special security precautions, to me or someone I designate, or to other health care providers, health plans and others involved in my treatment, payment for my treatment, or <**Dental Practice's**> health care operations. The patient information that may be emailed may include my x-rays, health history, diagnosis, treatment, and payment records.

I understand that:

- I do not have to sign this form.
- My treatment, payment, enrollment and eligibility for benefits will not be affected by my decision about signing this form.
- If I don't sign this form, <**Dental Practice**> may use other ways to send my information, such as U.S. Mail, or may ask me to send my information to third parties myself.
- There is some risk that emails and other electronic messages may be improperly acquired by hackers or received by unintended recipients. If that happens, the information may be redisclosed and no longer protected by privacy law.
- <**Dental Practice**> does not email such sensitive personal information as Social Security number, credit card number, mental health diagnosis, genetic information, alcohol/substance abuse, or positive HIV status unless the patient insists.

I can tell you in writing to stop emailing my patient information at any time, but if I do so, this will not affect emails that <**Dental Practice**> already sent before receiving my written instructions to stop.

Patient name (please print) _____

Signature: _____ Date: _____

Dental Team: Give a copy of this signed form to the patient. Save the original in the patient's file.

_____

{NAME OF PRACTICE}

Sample 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 ____/____/____, 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 SEND HEALTH INFORMATION ABOUT YOU

Your protected health information ("PHI") includes information relating to your mental or physical health and to the health care provided to you, including materials like your dental records, dental x-rays, and payment records. Some documents containing PHI may include such sensitive personal information as a Social Security number, credit card number, mental health diagnosis, genetic information, alcohol/substance abuse records, positive HIV status, and other kinds of sensitive information.

Sometimes our dental practice needs to send PHI to the patient or to someone else, such as a specialist. There are various ways to send PHI, including email and other electronic means. Our dental practice does not encrypt email or other electronic forms of communication.

There is a risk that unencrypted information may be acquired by hackers or received by unintended recipients. If you are concerned about the security of PHI that may be sent unencrypted, please let us know and we will send it a different way, which may include providing the information to you to deliver.

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.

Treatment. We may disclose your health information to a specialist providing treatment to you.

Payment. 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. 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 the authority by law to make health care decisions for you, we will treat that patient representative the same way we would treat you with respect to your health information.

Disaster Relief. We may use or disclose your health information to assist in disaster relief efforts.

Required by Law. We may use or disclose your health information when we are required to do so by law.

Public Health Activities. We may disclose your health information for public health activities, including disclosures to:

- Prevent or control disease, injury or disability;
- Report child abuse or neglect;
- Report reactions to medications or problems with products or devices;
- Notify a person of a recall, repair, or replacement of products or devices;
- Notify a person who may have been exposed to a disease or condition; or
- Notify the appropriate government authority if we believe a patient has been the victim of abuse, neglect, or domestic violence.

National Security. We may disclose to military authorities the health information of Armed Forces personnel under certain circumstances. We may disclose to authorized federal officials health information required for lawful intelligence, counterintelligence, and other national security activities. We may disclose to correctional institution or law enforcement official having lawful custody the protected health information of an inmate or patient.

Secretary of HHS. We will disclose your health information to the Secretary of the U.S. Department of Health and Human Services when required to investigate or determine compliance with HIPAA.

Worker's Compensation. We may disclose your PHI to the extent authorized by and to the extent necessary to comply with laws relating to worker's compensation or other similar programs established by law.

Law Enforcement. We may disclose your PHI for law enforcement purposes as permitted by HIPAA, as required by law, or in response to a subpoena or court order.

Health Oversight Activities. We may disclose your PHI to an oversight agency for activities authorized by law. These oversight activities include audits, investigations, inspections, and credentialing, as necessary for

licensure and for the government to monitor the health care system, government programs, and compliance with civil rights laws.

Judicial and Administrative Proceedings. If you are involved in a lawsuit or a dispute, we may disclose your PHI in response to a court or administrative order. We may also disclose health information about you in response to a subpoena, discovery request, or other lawful process instituted by someone else involved in the dispute, but only if efforts have been made, either by the requesting party or us, to tell you about the request or to obtain an order protecting the information requested.

Research. We may disclose your PHI to researchers when their research has been approved by an institutional review board or privacy board that has reviewed the research proposal and established protocols to ensure the privacy of your information.

Coroners, Medical Examiners, and Funeral Directors. We may release your PHI to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. We may also disclose PHI to funeral directors consistent with applicable law to enable them to carry out their duties.

Fundraising. We may contact you to provide you with information about our sponsored activities, including fundraising programs, as permitted by applicable law. If you do not wish to receive such information from us, you may opt out of receiving the communications.

Other Uses and Disclosures of PHI

Your authorization is required, with a few exceptions, for disclosure of psychotherapy notes, use or disclosure of PHI for marketing, and for the sale of PHI. We will also obtain your written authorization before using or disclosing your PHI for purposes other than those provided for in this Notice (or as otherwise permitted or required by law). You may revoke an authorization in writing at any time. Upon receipt of the written revocation, we will stop using or disclosing your PHI, except to the extent that we have already taken action in reliance on the authorization.

Your Health Information Rights

Access. You have the right to look at or get copies of your health information, with limited exceptions. You must make the request in writing. You may obtain a form to request access by using the contact information listed at the end of this Notice. You may also request access by sending us a letter to the address at the end of this Notice. If you request information that we maintain on paper, we may provide photocopies. If you request information that we maintain electronically, you have the right to an electronic copy. We will use the form and format you request if readily producible. We will charge you a reasonable cost-based fee for the cost of supplies and labor of copying, and for postage if you want copies mailed to you. Contact us using the information listed at the end of this Notice for an explanation of our fee structure.

If you are denied a request for access, you have the right to have the denial reviewed in accordance with the requirements of applicable law.

Disclosure Accounting. With the exception of certain disclosures, you have the right to receive an accounting of disclosures of your health information in accordance with applicable laws and regulations. To request an accounting of disclosures of your health information, you must submit your request in writing to the Privacy Official. If you request this accounting more than once in a 12-month period, we may charge you a reasonable, cost-based fee for responding to the additional requests.

Right to Request a Restriction. You have the right to request additional restrictions on our use or disclosure of your PHI by submitting a written request to the Privacy Official. Your written request must include (1) what information you want to limit, (2) whether you want to limit our use, disclosure or both, and (3) to whom you want the limits to apply. We are not required to agree to your request except in the case where the disclosure is to a health plan for purposes of carrying out payment or health care operations, and the information pertains solely to a health care item or service for which you, or a person on your behalf (other than the health plan), has paid our practice in full.

Alternative Communication. You have the right to request that we communicate with you about your health information by alternative means or at alternative locations. You must make your request in writing. Your request must specify the alternative means or location, and provide satisfactory explanation of how payments will be handled under the alternative means or location you request. We will accommodate all reasonable requests. However, if we are unable to contact you using the ways or locations you have requested we may contact you using the information we have.

Amendment. You have the right to request that we amend your health information. Your request must be in writing, and it must explain why the information should be amended. We may deny your request under certain circumstances. If we agree to your request, we will amend your record(s) and notify you of such. If we deny your request for an amendment, we will provide you with a written explanation of why we denied it and explain your rights.

Right to Notification of a Breach. You will receive notifications of breaches of your unsecured protected health information as required by law.

Electronic Notice. You may receive a paper copy of this Notice upon request, even if you have agreed to receive this Notice electronically on our Web site or by electronic mail (e-mail).

Questions and Complaints

If you want more information about our privacy practices or have questions or concerns, please contact us.

If you are concerned that we may have violated your privacy rights, or if you disagree with a decision we made about access to your health information or in response to a request you made to amend or restrict the use or disclosure of your health information or to have us communicate with you by alternative means or at alternative locations, you may complain to us using the contact information listed at the end of this Notice. You also may submit a written complaint to the U.S. Department of Health and Human Services. We will provide you with the address to file your complaint with the U.S. Department of Health and Human Services upon request.

We support your right to the privacy of your health information. We will not retaliate in any way if you choose to file a complaint with us or with the U.S. Department of Health and Human Services.

Our Privacy Official: _____

Telephone: _____ Fax: _____

Address: _____

E-mail: _____