PRACTICAL GUIDE SERIES

Chapter 2

25 Steps Toward Privacy and Breach Notification Compliance

What You Will Learn in This Chapter

- Understand 25 steps toward HIPAA privacy compliance
- Use the sample policies and procedures and sample forms as tools to help you tailor and update your dental practice's policies and procedures.
- Identify topics that must be addressed in training of your workforce members (including management).

Key Terms

Below are some key terms used in this chapter. See Appendix 1.1 for plain-language definitions and Appendix 1.2 official definitions of HIPAA terms.

HIPAA – When we refer to "HIPAA," we mean the HIPAA Privacy, Security and Breach Notification Rules.

Dental practice – When we refer to a "dental practice" we mean a dental practice that is a HIPAA covered entity. A dental practice is covered by HIPAA if it sends a "covered transaction," such as submitting a claim to a dental plan, in electronic form,[1] or if someone else (like a clearinghouse) sends an electronic covered transaction on behalf of the dental practice.[2]

Patient information – We use the term "patient information" in this book to mean "protected health information" ("PHI"). Most patient information is PHI, including dental records, health histories, billing records, radiographs, full-face photographs, and even "demographic" information such as patients' names, addresses, phone numbers, email addresses, genders, etc. For practical, everyday purposes, applying your HIPAA policies and procedures to any information about a patient is a good idea. But when you really need to figure out whether a specific piece of patient information is protected by HIPAA (for example, if you discover a suspected breach), the tools in Chapter 3 may help.

Patient – The HIPAA rules refer to "individuals." For a dental practice, this usually means the patient, and we use that term in this book. However, keep in mind that HIPAA protects information about both current and former patients, and that in some cases other people, such as a patient's legal representative, such as the parents or guardians of minor children, have rights under HIPAA.

The following terms are key to understanding the content of this chapter.

Breach
Business Associate
Contrary
Data Aggregation
Designated Record Set
De-identified
Disclosure
Electronic Media
Family Member
Genetic Information
Health Care Operations
Health Plan
Law Enforcement Official
Marketing
More Stringent
Payment
Privacy Official
Secured
Treatment
Use
Workforce

[1] In electronic form means: using electronic media, electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

[2] For more examples of covered transactions and information about covered entities, see the Covered Entity Charts from the Center for Medicare & Medicaid Services. They are available at *http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf*.

Appendix 2.1.1

Sample Designation of Privacy Official

This sample form illustrates how a dental practice might document its designation of the Privacy Official and make other documented personnel designations that the Privacy Rule requires.

_____

{NAME OF PRACTICE}

Effective _____ (date),

_____ (Name of Dental Practice)

designates _____ (name)

as:

- The Privacy Official, responsible for developing and implementing the dental practice's privacy policies and procedures, and as
- The person responsible for:
  - o receiving complaints
  - o providing further information about the Notice of Privacy Practices (for example, to patients, staff, etc.), and
  - o receiving and processing:
    - requests for access
    - accountings of disclosures
    - requests for amendment

Appendix 2.1.2
Sample Privacy Official Job Description

This sample form illustrates how a dental practice might write a job description for the Privacy Official.

General Duties:

Maintain the privacy of patient information and oversee activities that keep our practice in compliance with the HIPAA Privacy and Breach Notification Rule and applicable state laws on privacy, data security, and patient records.

Specific Duties:

The Privacy Official has the following specific duties:

- **Management Advisor**
  Work with the dental practice's management team and lawyers to comply with applicable federal and state laws. Stay current on privacy laws and updates in privacy technology. Immediately notify the Dentist[1] of any communication from or on behalf of a governing agency, such as the Office for Civil Rights or the state attorney general, (for example, if the dental practice receives a communication about a notice of investigation, compliance review, or audit).

- **Policies and Procedures**
  Develop, or serve as team leader in the development of, compliant privacy and breach notification policies and procedures. Implement the policies and procedures and integrate them into the practice's day-to-day activities.

- **Training and Sanctions**
  Provide timely training (planned courses, updates, reminders, and on-the-spot refreshers) to all workforce members, including management, employees, temps, trainees, volunteers, and others whose work for our dental practice is under the practice's direct control. Oversee sanctions for violations of HIPAA and our privacy policies and procedures according to our human resources policies, and bring any sanctions to the attention of the Dentist.

- **Risk Management**
  Collaborate with the Security Official to ensure that privacy and security risks are analyzed, documented and updated as appropriate.

- **Business Associates**
  Ensure that appropriate agreements are in place with each of our dental practice's business associates. Lead the practice in developing and updating business associate agreements and work with the management team and lawyers to develop and execute compliant business associate agreements.

- **Patient Rights**
  Respond to patient requests regarding their information and to questions about our privacy practices. Maintain documentation related to patient requests. Help the practice's employees understand how to respond appropriately to patient questions about their information and our privacy practices.

[1] In some larger practices or dental groups the person to be notified immediately is the Practice Administrator or Executive Director.

- **Documentation**
  Create, receive, and maintain documentation related to our privacy practices, and retain such documentation for six years from the date of its creation or the date when it last was in effect, whichever is later. Organize documentation for prompt retrieval in the event of a government investigation or audit.

- **Complaint Management**
  Receive, respond to, and document complaints about our privacy practices, investigating complaints and mitigating harm where appropriate. Educate workforce on our policies and procedures on complaints, and that retaliation and intimidation is prohibited against individuals who exercise their patient rights.

- **Qualifications**
  Must be familiar with dental and administrative functions of the practice; have excellent communication, problem solving, and research skills and an interest in privacy laws and regulations; be recognized as detail-oriented and having high integrity; have strong organizational skills and work well with management and staff.

Appendix 2.2

Sample Acknowledgement of Receipt of HIPAA Policies and Procedures

This sample form illustrates how a dental practice might obtain acknowledgement of receipt from each workforce member that he or she has received a copy (in paper or electronic format) of the practice's privacy, security and breach notification policies and procedures.

_____

{NAME OF PRACTICE}

I have received and reviewed a copy of our dental practice's privacy, security and breach notification policies and procedures.

I understand that I should ask our dental practice's Privacy Official if I have any questions about these policies and procedures.

Print Name: _____

Signature: _____

Date: _____

Apéndice 2.2b

Ejemplo de acuse de recibo de las políticas y los procedimientos de la HIPAA

Este formulario de ejemplo ilustra cómo un consultorio odontológico podría obtener acuse de recibo, por parte de cada miembro del personal, que indique que él o ella ha recibido una copia (en papel o en formato electrónico) de las políticas y los procedimientos de privacidad, seguridad y notificación de infracciones.

_____

{Nombre del consultorio}

He recibido de nuestro consultorio odontológico una copia de las políticas y los procedimientos de seguridad, privacidad y notificación de infracciones, y los he revisado.

Entiendo que, si tengo alguna duda respecto de estas políticas y estos procedimientos, debo consultar con el funcionario de privacidad de nuestro consultorio odontológico.

Nombre en letra de molde: _____

Firma: _____

Fecha: _____

Appendix 2.3.1

Sample Notice of Privacy Practices

The sample Notice of Privacy Practices presents examples of the information that HIPAA requires a covered dental practice to give to patients concerning the dental practice's privacy practices. A dental practice should consult a qualified attorney in the appropriate jurisdiction to determine the provisions that need to be included in the Notice of Privacy Practices in order to reflect the dental practice's particular privacy policies and to comply with any applicable state laws.

{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 in formation 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 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 (email).

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: _____

Email: _____

Appendix 2.3.1b Sample Notice of Privacy Practices – Spanish Version

{NOMBRE DEL CONSULTORIO}

Ejemplo de un Aviso de Prácticas de Privacidad

ESTE AVISO DESCRIBE CÓMO SU INFORMACIÓN MÉDICA PUEDE SER USADA Y DIVULGADA Y CÓMO USTED PUEDE TENER ACCESO A ESTA INFORMACIÓN. POR FAVOR, LÉALO DETENIDAMENTE.

Por ley, a nosotros se nos requiere mantener la privacidad de la información de salud protegida, entregarles a los pacientes un aviso de nuestros deberes legales y prácticas de privacidad en lo que respecta a la información de salud protegida, y notificarles a las personas afectadas después de cualquier acceso no autorizado a la información de salud protegida. Nosotros tenemos que cumplir las prácticas de privacidad descritas en este Aviso mientras esté en vigencia. Este Aviso entrará en vigencia en ____/____/____, y seguirá vigente hasta que lo reemplacemos.

Nos reservamos el derecho a cambiar nuestras prácticas de privacidad y los términos de este Aviso en cualquier momento, siempre y cuando tales cambios estén permitidos por las leyes que correspondan, y para establecer la vigencia de disposiciones nuevas en el Aviso para toda la información de salud protegida que mantenemos. Cuando hagamos un cambio significativo en nuestras prácticas de privacidad, nosotros cambiaremos este Aviso, colocaremos una copia del Aviso nuevo de manera clara y prominente en nuestro consultorio y proporcionaremos copias del Aviso nuevo cuando sean solicitadas.

Usted puede pedir una copia de nuestro Aviso en cualquier momento. Para obtener más información sobre nuestras prácticas de privacidad o copias adicionales de este Aviso, comuníquese con nosotros usando la información de contacto al final de este Aviso.

MANERAS EN LAS QUE PODEMOS USAR Y DIVULGAR SU INFORMACIÓN DE SALUD

Nosotros podemos usar y divulgar su información de salud para diferentes propósitos, entre ellos tratamiento, pago y operaciones de salud. A continuación hemos proporcionado una descripción y un ejemplo de cada una de estas categorías. Cierta información, como por ejemplo la relacionada con VIH, genética, los expedientes de abuso de alcohol y/o substancias y los expedientes de salud mental podrían contar con protecciones especiales de confidencialidad de conformidad con las leyes estatales o federales correspondientes. Nosotros cumpliremos con estas protecciones especiales en lo que respecta a casos aplicables que incluyan estos tipos de expedientes.

Tratamiento. Nosotros podemos usar y divulgar su información de salud para su tratamiento. Por ejemplo, podemos compartir su información de salud con un especialista que le esté proporcionando tratamiento.

Pagos. Nosotros podemos usar y divulgar su información de salud para obtener reembolso por el tratamiento y los servicios que usted reciba de nosotros o de otra entidad involucrada en su atención. Las actividades de pago incluyen facturación, cobro, manejo de reclamos y determinaciones de elegibilidad y cobertura a fin de obtener pago de usted, una compañía de seguros o un tercero. Por ejemplo, podemos enviarle reclamos a su plan dental que contendrán cierta información de salud.

Operaciones de salud. Nosotros podemos usar y divulgar su información de salud en conexión con nuestras operaciones de salud. Por ejemplo, operaciones de salud incluyen evaluaciones de calidad y actividades de mejoramiento, conducir programas de capacitación y actividades de licenciamiento.

Personas involucradas en su atención o responsables de pagar por su atención. Nosotros podemos compartir su información de salud con un familiar o amigo suyo o con cualquier otra persona que usted identifique porque está involucrada con su atención o es responsable por el pago de su atención. Además, podemos divulgar información con respecto a usted con un representante de paciente. Si una persona cuenta con autorización legal para tomar decisiones de atención médica por usted, nosotros trataremos a ese representante del paciente de la misma manera que lo trataríamos a usted en lo que respecta a su información de salud.

Asistencia en caso de desastres. Nosotros podemos usar o divulgar su información de salud para prestar ayuda en casos de desastre.

Requerido por ley. Nosotros podemos usar o divulgar su información de salud cuando sea requerido por ley.

Actividades de salud pública. Nosotros podemos divulgar su información de salud por razones de salud pública, y estas incluyen:

- Prevenir o controlar enfermedades, lesiones o discapacidad;
- Reportar abuso de niños o casos de negligencia;
- Reportar reacciones a medicamentos o problemas con productos o aparatos;
- Notificarle a una persona sobre productos o aparatos que se van a recolectar, reparar o reemplazar;
- Notificarle a una persona que puede haber estado expuesta a una enfermedad o condición; o
- Notificarle a la autoridad gubernamental correspondiente cuando creamos que un paciente ha sido víctima de abuso, negligencia o violencia doméstica.

Seguridad Nacional. Nosotros podemos divulgarle la información de salud del personal de las fuerzas armadas a las autoridades militares en ciertas circunstancias. Nosotros podemos divulgarle a los funcionarios federales autorizados la información que requieran para actividades legales de inteligencia, contrainteligencia o de otro tipo de seguridad nacional. Nosotros podemos divulgarle la información de salud protegida de un recluso o paciente a una institución correccional u oficial de policía que tenga custodia legal de esa persona.

Secretario del Departamento de Salud y Servicios Humanos. Nosotros le divulgaremos su información de salud al Secretario del Departamento de Salud y Servicios Humanos de Estados Unidos cuando sea requerido para investigar o determinar el cumplimiento de la Ley HIPAA.

Compensación obrera. Nosotros podemos divulgar su información de salud protegida hasta el grado autorizado por y necesario para cumplir las leyes relacionadas con la compensación obrera u otros programas similares establecidos por ley.

Ejecución de la ley. Nosotros podemos divulgar su información de salud protegida por motivos de ejecución de la ley según esté permitido por la Ley HIPAA, como sea requerido legalmente, o en respuesta a un emplazamiento u orden de tribunal.

Actividades de supervisión de salud. Nosotros podemos compartir su información de salud protegida con una agencia de supervisión para actividades autorizadas por ley. Estas actividades de supervisión incluyen auditorías, investigaciones, inspecciones y determinaciones de credenciales según sean necesarias para obtener licencia y para que el gobierno supervise el sistema de atención médica, los programas gubernamentales y el cumplimiento de las leyes de derechos civiles.

Procesos judiciales y administrativos. Si usted está involucrado en una demanda o disputa, nosotros podemos divulgar su información de salud protegida en respuesta a una orden de un tribunal o administrativa. También podemos divulgar su información de salud en respuesta a un emplazamiento, solicitud de descubrimiento u otros procesos de ley instituidos por otra persona involucrada en la disputa, pero únicamente si han habido esfuerzos por la parte que la está solicitando o por nosotros de decirle sobre la solicitud o de obtener una orden para proteger la información solicitada.

Investigación. Nosotros podemos compartir su información de salud protegida con investigadores cuando su investigación haya sido aprobada por una junta de revisión institucional o junta de privacidad que haya revisado la propuesta de investigación y establecido protocolos para asegurar la privacidad de su información.

Médicos forenses y directores fúnebres. Nosotros podemos compartir su información de salud protegida con un médico forense. Esto podría ser necesario, por ejemplo, para identificar a una persona fallecida o determinar la causa de muerte. Nosotros también podemos compartir su información de salud protegida con directores fúnebres de conformidad con las leyes aplicables para que ellos puedan llevar a cabo sus funciones.

Recaudación de fondos. Nosotros podemos comunicarnos con usted para darle información sobre actividades que auspiciamos, que incluyen programas de recaudación de fondos, según lo permitan las leyes aplicables. Si usted no desea recibir ese tipo de información de nosotros, puede optar por no recibir las comunicaciones.

OTROS USOS Y DIVULGACIONES DE LA INFORMACIÓN DE SALUD PROTEGIDA

Se requerirá su autorización (con pocas excepciones) para divulgar notas de sicoterapia, usar o divulgar la información de salud protegida para propósitos de mercadeo o vender la información de salud protegida. Nosotros también obtendremos su autorización por escrito antes de usar o divulgar su información de salud protegida para propósitos que no sean los dispuestos en este Aviso (o como de otro modo lo permitan o requieran las leyes). Usted puede revocar una autorización por escrito en cualquier momento. Al recibir la revocación por escrito, nosotros dejaremos de usar o divulgar su información de salud protegida excepto al grado que ya hayamos tomado acción habiendo contado con la autorización.

SUS DERECHOS EN CUANTO A LA INFORMACIÓN DE SALUD

Acceso. Usted tiene derecho a ver o conseguir copias de su información de salud con limitadas excepciones. Usted deberá solicitarlo por escrito. El formulario para solicitar acceso se puede obtener usando la información de contacto al final de este Aviso. Usted también puede solicitar acceso enviándonos una carta a la dirección al final de este Aviso. Si solicita información que tenemos en papel, nosotros podemos proporcionarle fotocopias. Si pide información que mantenemos de forma electrónica, usted tiene derecho a obtener una copia electrónica. Nosotros usaremos la forma y formato que usted pida si está disponible. Nosotros le cobraremos un cargo razonable basado en el costo de los suministros y el trabajo de hacer las copias, y por el franqueo si quiere que le enviemos las copias por correo. Comuníquese con nosotros usando la información al final de este Aviso para que le expliquemos nuestra estructura de cargos.

Si se le niega una solicitud de acceso, usted tiene derecho a que la denegación sea revisada de conformidad con los requisitos de las leyes aplicables.

Registro de divulgación. Excepto en el caso de ciertas divulgaciones, usted tiene derecho a recibir un registro de las veces que se ha divulgado su información de salud de conformidad con las leyes y regulaciones aplicables. Para pedir un registro de las divulgaciones de su información de salud, deberá presentarle una solicitud por escrito al Funcionario de Privacidad. Si usted solicita este registro más de una vez en un período de 12 meses, nosotros podemos cobrarle un cargo razonable basado en el costo por responder a las solicitudes adicionales.

Derecho a solicitar una restricción. Usted tiene derecho de solicitar restricciones adicionales a nuestro uso o divulgación de su información de salud protegida presentándole una solicitud por escrito al Funcionario de Privacidad. Su solicitud por escrito deberá incluir (1) qué información desea limitar, (2) si desea limitar nuestro uso, divulgación, o ambos, y (3) a quién quiere que le apliquen las limitaciones. **A nosotros no se nos requiere estar de acuerdo con su solicitud excepto en el caso en que la divulgación sea a un plan médico con el propósito de recibir un pago** o efectuar operaciones de salud, y la información es únicamente en referencia a un artículo o servicio de salud por el que usted, o una persona a nombre suyo (que no sea el plan médico) le haya pagado por completo a nuestro consultorio.

Comunicación alternativa. Usted tiene derecho de solicitar que nos comuniquemos con usted sobre su información de salud por un medio alternativo o en un lugar alternativo. Usted deberá solicitarlo por escrito. Su solicitud deberá especificar el medio o lugar alternativo, y proporcionar una explicación satisfactoria sobre cómo se manejarán los pagos en el medio o lugar alternativo que está solicitando. Nosotros acomodaremos toda solicitud razonable. Sin embargo, si no podemos comunicarnos con usted usando los medios o lugares que ha solicitado, entonces podremos comunicarnos con usted usando la información que tengamos.

Enmienda. Usted tiene derecho a pedir que enmendemos su información de salud. Su solicitud deberá ser por escrito, y la misma deberá explicar por qué la información debe ser enmendada. Nosotros podemos denegar su solicitud en ciertas circunstancias. Si estamos de acuerdo con su solicitud, enmendaremos su expediente y se lo notificaremos. Si denegamos su solicitud de enmienda, le proporcionaremos una explicación por escrito de por qué la negamos y explicaremos sus derechos.

Derecho a recibir notificación de acceso no autorizado. Usted recibirá notificaciones de cualquier acceso no autorizado a su información de salud protegida según se requiere por ley.

Aviso electrónico. Usted puede recibir una copia impresa de este Aviso si la solicita, aún cuando haya acordado recibir este Aviso electrónicamente en nuestro sitio Web o por correo electrónico (e-mail).

PREGUNTAS Y QUEJAS

Si desea más información sobre nuestras prácticas de privacidad o tiene preguntas o inquietudes, comuníquese con nosotros.

Si le preocupa que pudiéramos haber violado sus derechos de privacidad, o si no está de acuerdo con una decisión nuestra en cuanto al acceso a su información de salud o en respuesta a una solicitud suya para enmendar o restringir el uso o divulgación de su información de salud o para que nos comuniquemos con usted por un medio alternativo o a un lugar alternativo, usted puede presentarnos una queja al respecto usando la información de contacto al final de este Aviso. Usted también puede presentarle una queja por escrito al Departamento de Salud y Servicios Humanos de Estados Unidos. Nosotros le proporcionaremos la dirección para presentar su queja ante el Departamento de Salud y Servicios Humanos de Estados Unidos cuando la solicite.

Nosotros apoyamos su derecho a la privacidad de su información de salud. Nosotros no tomaremos ningún tipo de represalia si usted decide presentarnos una queja a nosotros o ante el Departamento de Salud y Servicios Humanos de Estados Unidos.

Nuestro Funcionario de Privacidad: _____

Teléfono: _____ Fax: _____

Dirección: _____

Correo electrónico: _____

Appendix 2.3.2

Sample Acknowledgement of Receipt of Notice of Privacy Practices

This sample form illustrates how a dental practice might obtain acknowledgement of receipt of its Notice of Privacy Practices or document its good faith effort to obtain that acknowledgement.

{NAME OF PRACTICE}

You May Refuse to Sign This Acknowledgment

I have received a copy of this office's Notice of Privacy Practices.

Print Name: _____

Signature: _____

Date: _____

For Office Use Only

We attempted to obtain written acknowledgement of receipt of our Notice of Privacy Practices, but acknowledgement could not be obtained because:

- ☐ Individual refused to sign
- ☐ Communications barriers prohibited obtaining the acknowledgement
- ☐ An emergency situation prevented us from obtaining acknowledgement
- ☐ Other (Please Specify)

_____

_____

_____

Apéndice 2.3.2b

Ejemplo de acuse de recibo del Aviso de Prácticas de Privacidad

Este formulario de ejemplo ilustra cómo un consultorio odontológico puede obtener un acuse de recibo de su Aviso de Prácticas de Privacidad o documentar el esfuerzo realizado de buena fe para obtener ese acuse de recibo.

_____

{Nombre del consultorio}

Usted puede rehusarse a firmar este acuse de recibo

He recibido una copia del Aviso de Prácticas de Privacidad de este consultorio.

Nombre en letra de molde: _____

Firma: _____

Fecha: _____

_____

Para uso interno solamente

Intentamos obtener un acuse de recibo por escrito de nuestro Aviso de Prácticas de Privacidad, pero no pudimos obtenerlo por el siguiente motivo:

- ☐ La persona se negó a firmar.
- ☐ Hubo barreras de comunicación que impidieron la obtención del acuse de recibo.
- ☐ Una situación de emergencia nos impidió obtener el acuse de recibo.
- ☐ Otro (especifique)

_____

_____

_____

Appendix 2.4
Sample List of Designated Record Sets

This sample form illustrates how a dental practice might write a list of designated record sets.

This list was created on_____ , 20 _____,

and was in effect until _____ , 20 _____.

Name of the record set	Location of the record set

Appendix 2.5.1

Sample Workforce Access to Patient Information

This sample form illustrates how a dental practice might document authorized workforce access to patient information.

This document was created on _____ , 20 _____,

and was in effect until _____ , 20 _____.

Name of workforce member or group	Patient information needed to do the job	Any conditions that apply to access

Appendix 2.5.2
Sample Routine Disclosures and Requests

This sample form illustrates how a dental practice might document minimum necessary levels for routine disclosures and requests.

For use when our dental practice makes a routine disclosure of patient information to a third party

This list was created on _____, 20 _____,
and was in effect until _____, 20 _____.

Type of routine disclosure	Patient information that may be disclosed without checking with the Privacy Official

For use when our dental practice makes a routine request for patient information from a third party

This list was created on _____, 20 _____,
and was in effect until _____, 20 _____.

Type of routine request for patient information	Patient information that may be requested without checking with the Privacy Official

Minimum necessary does not apply in the following situations:

- Disclosing patient information to a health care provider for treatment
- Requesting patient information from a health care provider for treatment
- Disclosing a patient's information to the patient
- When a patient has signed an authorization form for the use or disclosure
- Disclosures to the U.S. Department of Health and Human Services
- Uses and disclosures required by law
- Uses and disclosures required in order to comply with the Privacy Rule

Unless one of the above exceptions applies, our dental practice will not access, use, disclose or request a patient's entire dental record unless the entire dental record is needed to accomplish the purpose of the use, disclosure or request.

Appendix 2.6
Sample Verification of Identity

This sample form illustrates how a dental practice might document the verification of the identity and authority of a person requesting patient information.

Please provide us with the following information.

Name of patient whose information you are requesting:

_____

Patient's Date of Birth: _____

The specific patient information that you are requesting: _____

_____

Your Name: _____

Address: _____

City: _____ State: _____ Zip: _____

Describe your authority to access this information:

_____

If you are a patient's personal representative:

Relationship to Patient: _____

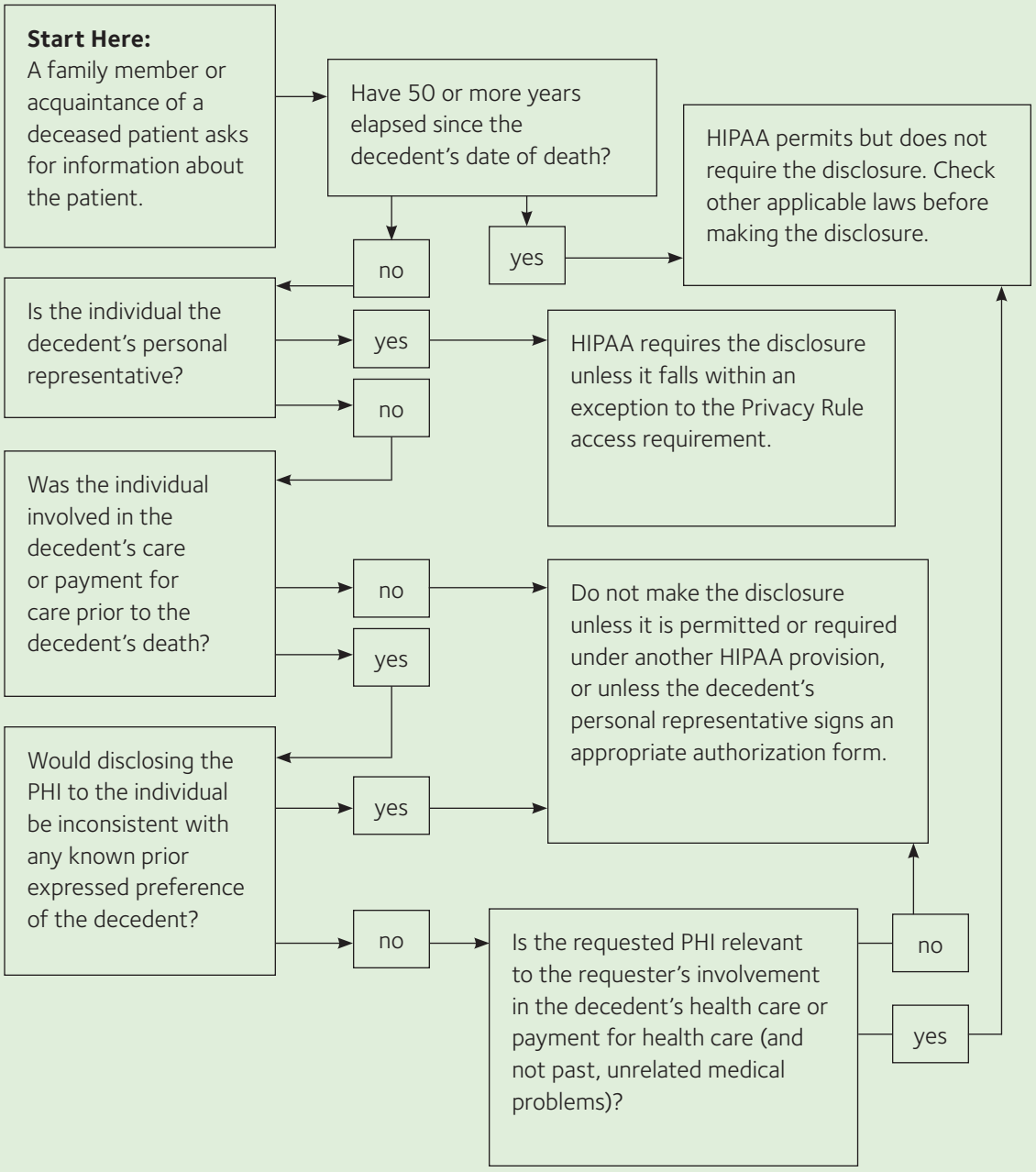
I certify that the above information is correct.

Signature: _____ Date: _____

Dental Staff: Describe documentation presented by the requester:

_____

Appendix 2.8
Sample Decision Tree: Decedent PHI



Appendix 2.9

Sample Authorization Form for Use or Disclosure of Patient Information

This sample form illustrates how a dental practice might obtain and document authorization for a use or disclosure of patient information that is not permitted or required by HIPAA.

Patient Name: _____

Patient's Date of Birth: _____ Patient's Chart No.: _____

I hereby authorize the use and disclosure of the patient information as described below. I understand that information disclosed pursuant to this authorization may be subject to redisclosure by the recipient and may no longer be protected by HIPAA Privacy regulations.

Specific description of the patient information to be used or disclosed:

_____

_____

Purpose(s) of this use or disclosure: _____

[If the patient or the patient's personal representative is requesting the use or disclosure, you may write "at the request of the individual" for the purpose.]

I authorize the following person(s) to make this use or disclosure:

_____

_____

The following person(s) may receive this patient information:

_____

[If this authorization is required for a use or disclosure of patient information for a subsidized marketing communication, add "I understand that the dental practice will receive financial remuneration for making this marketing communication."]

[If this authorization is required for a sale of patient information, add "I understand that this disclosure will result in remuneration to the dental practice."]

I understand that I may revoke this authorization at any time, and that my revocation is not effective unless it is in writing and received by the dental practice's Privacy Official at _____ _____. **[Insert address of the Privacy Official (or other person at the dental office responsible for patient authorizations). If the description of how to revoke an authorization is in the Notice of Privacy Practice, replace the first sentence of this paragraph with "I understand that I may revoke this authorization at any time by following the directions in the Notice of Privacy Practices. I understand that my revocation must be in writing."]** If I revoke this authorization, my revocation will not affect any actions taken by the dental practice before receiving my written 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. **[If an exception to the prohibition on conditioning authorizations applies, delete this sentence and insert a description of the consequences to the patient of a refusal to sign the authorization.]**

This authorization expires on the following date, or when the following event occurs:

_____

[Expiration events must relate to the patient or to the purpose of the use or disclosure. If the authorization is for research, the expiration may state "end of the research study," "none," or similar language.]

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: _____

Apéndice 2.9b

Ejemplo de formulario de autorización para el uso o la divulgación de información del paciente

Este formulario de ejemplo ilustra como un consultorio odontológico podría obtener y documentar una autorización para un uso o una divulgación de información del paciente que no están permitidos ni requeridos por HIPAA.

Nombre del paciente: _____

Fecha de nacimiento del paciente: _____

N.º de expediente del paciente:_____

Por el presente, autorizo el uso y la divulgación de la información del paciente según se describe a continuación. Entiendo que la información que se divulgue de conformidad con esta autorización puede estar sujeta a una nueva divulgación por parte del receptor y puede ya no estar protegida por los reglamentos de privacidad de la HIPAA.

Descripción específica de la información del paciente, que se va a utilizar o divulgar:

_____

_____

Propósito(s) de este uso o esta divulgación:_____

[Si el paciente o el representante personal del paciente está solicitando el uso o la divulgación, puede escribir "a petición de la persona" como propósito.]

Autorizo a la(s) siguiente(s) persona(s) a realizar este uso o esta divulgación:

_____

_____

Las siguientes personas pueden recibir esta información del paciente:

_____

[Si esta autorización se requiere para un uso o una divulgación de la información del paciente para una comunicación de marketing subsidiado, debe agregarse "Entiendo que el consultorio odontológico recibirá remuneración financiera por realizar esta comunicación de marketing"].

[Si esta autorización se requiere para una venta de la información del paciente, debe agregarse "Entiendo que esta divulgación dará lugar a una remuneración para el consultorio odontológico"].

Entiendo que puedo revocar esta autorización en cualquier momento, y que mi revocación no se hará efectiva a menos que sea por escrito y la haya recibido el funcionario de privacidad del consultorio en _____. **[Insertar el domicilio del funcionario de privacidad (o de la persona responsable de las autorizaciones de los pacientes del consultorio odontológico). Si la descripción de cómo revocar una autorización está en el Aviso de Prácticas de Privacidad, reemplace la primera frase de este párrafo con "Entiendo que puedo revocar esta autorización en cualquier momento siguiendo las instrucciones que figuran en el Aviso de Prácticas de Privacidad. Entiendo que mi revocación debe ser por escrito"].** Si revoco esta autorización, mi revocación no afectará ninguna acción tomada por el consultorio odontológico antes de recibir mi revocación por escrito.

Entiendo que puedo negarme a firmar esta autorización y que mi negativa a firmar no afectará de ninguna manera mi tratamiento, pago, inscripción en un plan de salud ni mi elegibilidad para recibir beneficios. **[Si corresponde una excepción a la prohibición de autorizaciones con condicionamientos, elimine esta oración e inserte una descripción de las consecuencias para el paciente si se niega a firmar la autorización].**

Esta autorización vence en la fecha indicada a continuación, o cuando ocurra el siguiente evento:

_____

[Los eventos de vencimiento deben estar relacionados con el paciente o con el propósito del uso y la divulgación. Si la autorización es para investigación, la fecha de vencimiento debe indicar "final del estudio de investigación", "ninguna", o un texto similar].

Firma del paciente o del representante personal del paciente:

_____Fecha: _____

Si es el representante personal:

Nombre en letra de molde: _____

Firma: _____

Relación con el paciente: _____

_____

PARA USO INTERNO SOLAMENTE

_____

Se le entregó copia de la autorización firmada a la persona:

Fecha: _____

Iniciales: _____

Appendix 2.10.1

Sample Patient Authorization for Marketing – All Products and Services

This sample form illustrates how a dental practice might obtain patient authorization for the use or disclosure of the patient's information for an appropriate subsidized marketing communication. The following authorization applies to subsidized communications generally. The scope of an authorization may apply more narrowly to communications about a single product or service (see form 2.10.2), or to the products or services of a single company (see form 2.10.3). Note that this sample form does not apply to the sale of patient information (Chapter 2, Step 11).

To our Patients:

From time to time, our dental practice would like to tell patients about products and services that we think may be of interest to them.

When we give patients promotional gifts of nominal value, or recommend products or services in face-to-face communications, we do not require the patient's written authorization. However, we do require a patient's written authorization before sending other kinds of marketing communications if our dental practice receives financial remuneration for sending the communication.

If you would like to receive information about products and services from our dental practice, please complete and sign the authorization form below and return it to us at your convenience.

Authorization

Patient Name: _____

Patient's Date of Birth: _____ Patient's Chart No.: _____

I hereby authorize the dental practice to use my name and address and other information about my dental health to provide marketing communications to me. I also authorize the dental practice to disclose such information to a business associate for purposes of sending marketing communications to me.

I understand that the dental practice receives financial remuneration for making marketing communications.

I understand that information disclosed pursuant to this authorization may be subject to redisclosure by the recipient and may no longer be protected by HIPAA Privacy regulations.

I understand that I may revoke this authorization at any time, and that my revocation is not effective unless it is in writing and received by the dental practice's Privacy Official at the following address:

_____

[If the description of how to revoke an authorization is in the Notice of Privacy Practice, replace the first sentence of this paragraph with "I understand that I may revoke this authorization at any time by following the directions in the Notice of Privacy Practices. I understand that my revocation must be in writing."]

I understand that if I revoke this authorization, my revocation will not affect any actions taken by the dental practice before receiving my written 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 the following date, or when the following event occurs:

_____

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:_____

Appendix 2.10.2

Sample Patient Authorization for Marketing – Single Product or Service

This sample form illustrates how a dental practice might obtain patient authorization for the use or disclosure of the patient's information for an appropriate subsidized marketing communication. The following authorization applies to subsidized communications about a single product or service. The scope of an authorization may apply more broadly to the products or services of a single company (see form 2.10.3) or to marketing communications generally (see form 2.10.1). Note that this sample form does not apply to the sale of patient information (Chapter 2, Step 11).

To our Patients:

Our dental practice would like to tell our patients about a new product [or service] that we think may be of interest to them: _____ [insert name of product or service].

When we give patients promotional gifts of nominal value, or recommend products or services in face-to-face communications, we do not require the patient's written authorization. However, we do require a patient's written authorization before sending other kinds of marketing communications if our dental practice receives financial remuneration for sending the communication.

If you would like to receive information about this product [or service] from our dental practice, please complete and sign the authorization form below and return it to us at your convenience.

Authorization

Patient Name: _____

Patient's Date of Birth:_____ Patient's Chart No.: _____

I hereby authorize the dental practice to use my name and address and other information about my dental health to provide marketing communications to me about the product or service described above. I also authorize the dental practice to disclose such information to a business associate for purposes of sending such marketing communications to me.

I understand that the dental practice will receive financial remuneration for making this marketing communication.

I understand that information disclosed pursuant to this authorization may be subject to redisclosure by the recipient and may no longer be protected by HIPAA Privacy regulations.

I understand that I may revoke this authorization at any time, and that my revocation is not effective unless it is in writing and received by the dental practice's Privacy Official at the following address:

_____

[If the description of how to revoke an authorization is in the Notice of Privacy Practice, replace the first sentence of this paragraph with "I understand that I may revoke this authorization at any time by following the directions in the Notice of Privacy Practices. I understand that my revocation must be in writing."]

I understand that if I revoke this authorization, my revocation will not affect any actions taken by the dental practice before receiving my written 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 the following date, or when the following event occurs:

_____

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:_____

Appendix 2.10.3

Sample Patient Authorization for Marketing – Single Company

This sample form illustrates how a dental practice might obtain patient authorization for the use or disclosure of the patient's information for an appropriate subsidized marketing communication. The following authorization applies to subsidized communications about a single company's products and/or services. The scope of an authorization may apply more narrowly to a single product or service (see form 2.10.2) or more broadly to marketing communications generally (see form 2.10.1). Note that this sample form does not apply to the sale of patient information (Chapter 2, Step 11).

To our Patients:

Our dental practice would like to tell our patients about products [and/or services] from

_____

[insert name of company] that we think may be of interest to them.

When we give patients promotional gifts of nominal value, or recommend products or services in face-to-face communications, we do not require the patient's written authorization. However, we do require a patient's written authorization before sending other kinds of marketing communications if our dental practice receives financial remuneration for sending the communication.

If you would like to receive information from our dental practice about _____'s [insert name of company] products [and/or services], please complete and sign the authorization form below and return it to us at your convenience.

Authorization

Patient Name: _____

Patient's Date of Birth:_____ Patient's Chart No.: _____

I hereby authorize the dental practice to use my name and address and other information about my dental health to provide marketing communications to me about the products or services described above. I also authorize the dental practice to disclose such information to a business associate for purposes of sending such marketing communications to me.

I understand that the dental practice will receive financial remuneration for making this marketing communication.

I understand that information disclosed pursuant to this authorization may be subject to redisclosure by the recipient and may no longer be protected by HIPAA Privacy regulations.

I understand that I may revoke this authorization at any time, and that my revocation is not effective unless it is in writing and received by the dental practice's Privacy Official at the following address:

_____

[If the description of how to revoke an authorization is in the Notice of Privacy Practice, replace the first sentence of this paragraph with "I understand that I may revoke this authorization at any time by following the directions in the Notice of Privacy Practices. I understand that my revocation must be in writing."]

If I revoke this authorization, my revocation will not affect any actions taken by the dental practice before receiving my written 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 the following date, or when the following event occurs:

_____

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:_____

Appendix 2.13

Sample Business Associate Agreement

This sample form illustrates how a dental practice might enter into a business associate agreement with a business associate who will perform a service for the dental practice that involves access to patient information.

This sample business associate agreement is intended as only a tool to help dental practices comply with HIPAA. The sample provisions address only HIPAA requirements, not the underlying agreement between the parties, nor do these sample provisions address state law requirements. The sample may not be sufficient to create a binding contract under state law, and may not be compliant with applicable state law that is more stringent than HIPAA. Use of this sample agreement does not replace consultation with a lawyer or negotiations between the dental practice and business associate. Words or phrases contained in bold brackets (**[like this]**) are intended as optional language for dental practices using this sample agreement.

Sample Business Associate Agreement

This Business Associate Agreement (this "Agreement") is entered into as of

_____ , 20_____ , (the "Effective Date") by and between

_____ ("Dental Practice")

and _____("Business Associate").

RECITALS:

WHEREAS, Business Associate performs services for or on behalf of Dental Practice (the "Services") pursuant to that certain _____ Agreement dated _____, 20____ (the "Underlying Agreement"), which Services involve the access, use and/or disclosure of Protected Health Information (as defined below); and

WHEREAS, the parties desire to enter into this Agreement in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations, as amended and in effect.

NOW THEREFORE, the parties agree as follows:

1. Definitions. Capitalized terms not otherwise defined in this Agreement shall have the same meaning as those terms in the HIPAA Privacy Rule and Security Rule (as defined below).

(a) "Breach," when capitalized, shall have the meaning set forth in 45 CFR § 164.402 (including all of its subsections).

(b) "Electronic Protected Health Information" or "EPHI" shall have the same meaning as the term "electronic protected health information" in 45 CFR § 160.103, limited to information that Business Associate creates, accesses, receives or maintains for or on behalf of Dental Practice.

(c) "Protected Health Information" or "PHI" shall have the meaning set forth in in 45 CFR § 160.103, limited to information that Business Associate creates, accesses, receives or maintains for or on behalf of Dental Practice. PHI includes EPHI.

(d) "Privacy Rule" means the Standards for Privacy of Individually Identifiable Health Information, codified at 45 CFR parts 160 and 164, Subparts A, D and E, as currently in effect.

(e) "Security Rule" means the Standards for Security for the Protection of Electronic Protected Health Information, codified at 45 CFR parts 160 and 164, Subparts A and C, as currently in effect.

(f) "Unsecured Protected Health Information" shall have the same meaning as the term "unsecured protected health information" in 45 CFR § 164.402, limited to such information accessed, created, received or maintained by Business Associate.

2. Scope of Use and Disclosure of PHI.

(a) Business Associate Status. Business Associate acknowledges that it is Dental Practice's "business associate" as defined by HIPAA. Business Associate agrees to comply with the HIPAA regulations as they directly apply to business associates.

(b) Performance of Service. Business Associate shall not access, use or further disclose PHI other than as permitted or required by this Agreement, to perform the Services pursuant to the Underlying Agreement or as Required by Law. Business Associate shall not access, use or disclose PHI in any manner that would violate HIPAA if such access, use or disclosure was done by Dental Practice.

[1. Uses and Disclosures Permitted By Law. Business Associate may use or disclose PHI: (A) as is necessary for the proper management and administration of Business Associate's organization, and (B) to carry out the legal responsibilities of Business Associate; provided, however, that any permitted disclosure of PHI to a third party must be either Required By Law or subject to reasonable assurances obtained by Business Associate from the third party that PHI will be held confidentially, and securely, and used or disclosed only as Required By Law or for the purposes for which it was disclosed to such third party, and that any breaches of confidentiality of PHI which become known to such third party will be immediately reported to Business Associate.]

[2. Statistical Aggregation. Business Associate shall not use PHI for any compilation or aggregation of data or for any commercial purpose whatsoever not set forth in this Agreement, unless permitted by Dental Practice in a written document.]

[3. De-identification. Business Associate shall not use PHI to create de-identified PHI for any purpose not set forth in this Agreement, unless permitted by Dental Practice in a written document.]

(c) Minimum Necessary. Business Associate shall not access, use or disclose more than the minimum necessary PHI to perform or fulfill the intended permissible purpose, in accordance with this Agreement.

(d) Privacy Rule. To the extent Business Associate carries out one or more of Dental Practice's obligations under the HIPAA Privacy Rule, Business Associate shall comply with the requirements of HIPAA that apply to Dental Practice in the performance of such obligation(s).

(e) Security Rule and Safeguards. Business Associate shall use safeguards that are appropriate and sufficient to prevent access, use or disclosure of PHI other than as permitted or required by this Agreement. Business Associate shall comply with the Security Rule with respect to EPHI, including implementing Administrative Safeguards, Physical Safeguards, and Technical Safeguards that reasonably and appropriately protect the Confidentiality, Integrity and Availability of EPHI.

(f) Notification. Without unreasonable delay, Business Associate shall notify Dental Practice, in writing, of any use or disclosure of PHI not provided for by this Agreement of which Business Associate becomes aware. Without unreasonable delay, Business Associate shall report to Dental Practice in writing of any Security Incident of which it becomes aware in accordance with the Security Rule and Business Associate's obligations under the same. Upon Dental Practice's request, Business Associate shall provide a report of any and all impermissible uses, disclosures and/or Security Incidents.

(g) Subcontractors. Business Associate shall ensure that any and all subcontractors that create, receive, maintain or transmit PHI on behalf of Business Associate agree, in writing, to the same restrictions and conditions that apply to Business Associate. Each subcontract agreement must include, without limitation, the provisions of this Agreement. Business Associate shall make such agreements with its subcontractors available to Dental Practice upon request.

(h) Audit. Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Dental Practice available to the Secretary of Health and Human Services and/or Dental Practice, upon request, for purposes of determining and facilitating Dental Practice's compliance with HIPAA.

(i) Patient Rights.

1. Patient Right to Review. Business Associate shall make PHI maintained in a Designated Record Set available to Dental Practice or, at the direction of Dental Practice, to an Individual, in accordance with §164.524 of the Privacy Rule.

2. Patient Right to Amend. Business Associate shall make PHI available for amendment and incorporate any amendments to PHI maintained in a Designated Record Set at the direction of Dental Practice and in accordance with §164.526 of the Privacy Rule. Dental Practice shall be involved in any decision of Business Associate to amend the PHI of an Individual.

3. Patient Right to Request Accounting. Business Associate shall document and make available to Dental Practice or, at the direction of Dental Practice, to an Individual, information relating to such Individual as is necessary for Dental Practice to respond to a request for an accounting of disclosures in accordance with §164.528 of the Privacy Rule.

   A. Business Associate agrees to implement an appropriate record-keeping process to ensure compliance with the requirements of this Section.

   B. Business Associate agrees to provide PHI it maintains electronically in a Designated Record Set in an electronic form at the request of Dental Practice or an Individual.

4. Notice to Dental Practice. Business Associate shall notify Dental Practice immediately in writing upon receiving a request from an Individual to review, copy or amend his or her medical record information or to receive an accounting of disclosures. Business Associate shall also provide Dental Practice with a prompt written report of the details of its handling of such requests.

(j) Breach. Business Associate shall notify Dental Practice of breaches of unsecured PHI in accordance with the requirements of 45 CFR § 164.410. Such notification shall include, to the extent possible, the identification of each Individual whose PHI has been or is reasonably believed to have been accessed, acquired, used or disclosed during the Breach, along with any other information that Dental Practice will be required to include in its notification to an affected Individual, the media and/or the Secretary, as applicable, including, without limitation, a description of the Breach, the date of the Breach and its discovery, the types of Unsecured Protected Health Information involved and a description of Business Associate's investigation, mitigation and prevention efforts.

(k) Mitigation. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate or a subcontractor or agent of Business Associate in violation of the requirements of this Agreement, the Privacy Rule, the Security Rule or other applicable federal or state law.

3. [Dental Practice Obligations.]

[(a) Notice of Privacy Practices. Dental Practice shall notify Business Associate of limitation(s) in its notice of privacy practices to the extent such limitation affects Business Associate's permitted uses or disclosures under this Agreement.]

[(b) Individual Authorization. Dental Practice shall notify Business Associate of changes in, or revocation of, authorization by an Individual to use or disclose PHI, to the extent such changes affect Business Associate's permitted uses or disclosures under this Agreement.]

[(c) Restrictions. Dental Practice shall notify Business Associate of restriction(s) in the use or disclosure of PHI that Dental Practice has agreed to, to the extent such restriction affects Business Associate's permitted uses or disclosures under this Agreement.]

4. Term and Termination.

(a) Term. The Term of this Agreement shall become effective as of the Effective Date, and remain in effect until all PHI is returned or destroyed in accordance with this Section.

(b) Termination for Cause. Dental Practice may terminate this Agreement immediately if Dental Practice, in its sole discretion, determines that Business Associate has violated a material term of this Agreement. Dental Practice, at its option and within its sole discretion, may (1) permit Business Associate take steps to cure the breach; and (2) in the event Dental Practice determines such cure is sufficient, elect to keep this Agreement in force.

(c) Obligations of Business Associate Upon Termination. Upon termination of this Agreement for any reason, Business Associate shall promptly return to Dental Practice or destroy all PHI received from Dental Practice, or created or received by Business Associate on behalf of Dental Practice, that Business Associate still maintains in any form. Business Associate shall retain no copies of the PHI in any form. Upon request by Dental Practice, Business Associate shall promptly supply a certification executed by an officer (vice president level or above) of the Business Associate confirming that Business Associate has returned or destroyed all PHI and all copies thereof.

(d) Survival. The obligations of Business Associate under this Section shall survive the termination of this Agreement.

5. [Limitation of Liability, Indemnification and Insurance.]

[(a) Limitation of Liability. To the extent that Business Associate has limited its liability under the terms of the Underlying Agreement, whether with a maximum recovery for direct damages or a disclaimer against any consequential, indirect or punitive damages, or other such limitations, all limitations shall exclude damages to Dental Practice arising out of a breach of this Agreement by Business Associate or any Breach of PHI by Business Associate.]

[(b) Indemnification. Business Associate agrees to indemnify, defend, and hold harmless Dental Practice and its directors, officers, affiliates, employees, agents, and permitted successors from and against any and all claims, losses, liabilities, damages, costs, and expenses (including reasonable attorneys' fees) arising out of or related to Business Associate's breach of its obligations under this Agreement, including, but not limited to a Breach of Unsecured Protected Health Information by Business Associate.]

[(c) Insurance. Business Associate agrees at the request of Dental Practice, to obtain and maintain insurance coverage against the improper use and disclosure of PHI by Business Associate, naming Dental Practice as a named insured. Promptly following a request by Dental Practice for the maintenance of such insurance coverage, Business Associate will provide a certificate evidencing such insurance coverage.]

6. Miscellaneous Provisions.

(a) Notices. Any notice required or permitted under this Agreement will be given in writing and will be sent —

to Dental Practice at: _____
_____
_____

to Business Associate at: _____
_____
_____

Notices will be deemed to have been received upon actual receipt, one business day after being sent by overnight courier service, or three business days after mailing by first-class mail, whichever occurs first.

(b) Governing Law. This Agreement will be governed by, and construed in accordance with the laws of the state of [STATE] without giving effect to choice of law provisions thereof.

(c) Waiver. No delay or omission by either party to exercise any right or remedy under this Agreement will be construed to be either acquiescence or the waiver of the ability to exercise any right or remedy in the future. Failure of a party to insist upon strict adherence to any term or condition of this Agreement shall not be considered a waiver by that party of its right thereafter to insist upon strict adherence to that, or any other, term or condition of this Agreement. No waiver of any breach of any provision of this Agreement shall constitute a waiver of any prior, concurrent or subsequent breach of the same or any other provisions hereof, and no waiver shall be effective unless made in writing and signed by an authorized representative of the waiving party.

(d) Severability. All provisions of this Agreement are separate and divisible, and if any part or parts of this Agreement are held to be unenforceable, the remainder of this Agreement will continue in full force and effect.

(e) Amendments. The parties shall amend this Agreement from time to time by mutual written agreement in order to keep this Agreement consistent with any changes made to the HIPAA laws or regulations in effect as of the Effective Date and with any new regulations promulgated under HIPAA. Dental Practice may terminate this Agreement and, where appropriate, the Underlying Agreement in whole or in part if the parties are unable to agree to such changes by the compliance date for such new or revised HIPAA laws or regulations.

(f) Interpretation. In the event of any conflict between the provisions of this Agreement and the Underlying Agreement, the provisions of this Agreement shall control. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the parties to comply with HIPAA.

(g) Automatic Amendment. This Agreement shall automatically incorporate any change or modification of applicable state or federal law as of the effective date of the change or modification. Business Associate agrees to maintain compliance with all changes or modifications to applicable state or federal law.

(h Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

(i) Independent contractor. The parties acknowledge and agree that Business Associate is an independent contractor. Nothing in this agreement shall be construed to create any partnership, joint venture, agency, or employment relationship of any kind between the parties. Notwithstanding the foregoing, to the extent that Business Associate is ever determined for any purpose to be an agent of the Dental Practice (under the Federal common law of agency or otherwise), Business Associate shall be acting outside of the scope of agency if Business Associate fails to notify the Dental Practice immediately if Business Associate violates or breaches any provision of this Agreement or violates the HIPAA Rules.

IN WITNESS WHEREOF, the parties have executed this Business Associate Agreement as of the Effective Date.

DENTAL PRACTICE	**BUSINESS ASSOCIATE**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____

Appendix 2.14.1

Sample Request for Access

This sample form illustrates how a dental practice might document a request for access to patient information.

Privacy Official Name: _____ Telephone: _____

Patient's Name (print): _____

Date of Birth: _____ (for identification purposes)

Describe the records you wish to access and the approximate dates of the records: _____

_____

_____

What would you like for us to do for you?

- ☐ I wish to see the requested records.
- ☐ I wish to get a copy of the requested records.
- ☐ I wish to see and get a copy of the requested records.
- ☐ If the requested records are in an electronic designated record set, I wish an electronic copy of the requested records the following form and format, if readily producible: _____

  _____

  If you would like the information emailed, enter the email address here (PLEASE PRINT VERY CLEARLY!): _____@_____

  We do not recommend sending patient information in an unencrypted email because third parties may be able to access the email.
- ☐ I want you to prepare summary of the requested records and I agree in advance to pay a fee in the amount of $_____.
- ☐ I want you to prepare an explanation of the records that I saw or got a copy of, and I agree in advance to pay a fee in the amount of $_____.
- ☐ I want you to send the copy of the requested records to:

  Name: _____

  Address: _____

Fees

Our practice charges a reasonable, cost-based fee to for copies of patient information, and for postage to mail records if requested.

Questions?
Please contact our privacy official listed at the top of this page if you have any questions about your request to inspect or copy records.

If the request is by a patient:

Patient Signature: _____ Date:_____

If the request is by a patient's personal representative:

Print the Name of the Personal Representative:_____

Relationship to the Patient: _____

I certify that I have the legal authority under federal and state laws to make this request on behalf of the patient identified above.

Signature of Personal Representative:

_____ Date:_____

For Dental Office Use Only

☐ Request for access denied (attach written denial).
☐ Request for access approved.

Appendix 2.14.2.1
Sample Request for Amendment

This sample form illustrates how a dental practice might document a patient's request to amend the patient's protected health information in the practice's designated record set.

To the Patient: Please use this form to ask our dental practice to change any information about you in our records. All requests for changes to our records must be in writing and must state the reason for the change. You must return this form to the Privacy Official listed on the bottom of this form.

Patient Information

Name of Patient (print name): _____

Patient's Date of Birth: _____ Today's Date: _____

Patient Signature: _____ Date: _____

For Personal Representative of the Patient:

Your Name: _____

Your Relationship to Patient: _____

Personal Representative Signature: _____ Date: _____

I hereby certify that I have legal authority under applicable law to make this request on behalf of the patient identified above.

Signature of Personal Representative: _____ Date: _____

Requested Amendment

Please describe in detail how you want your records changed: _____

_____

_____

Reason for requested change: _____

_____

Contact Person

Please contact the dental practice's Privacy Official if you have any questions relating to your request to amend records.

Privacy Official Name: _____

Address: _____

Telephone Number: _____

Appendix 2.14.2.2
Sample Denial of Request to Amend

This sample form illustrates how a dental practice might notify a patient that the dental practice has denied the patient's request to amend information in a designated record set.

Patient's Name: _____

Patient's Address: _____

Name of person who requested the change: _____

Dear _____ ,

We are responding to your request to amend patient information. We have reviewed the request carefully and we have determined that we cannot approve the amendment that you asked for.

This is the reason for that we cannot approve the amendment:

- ☐ The information or record is not in a designated record set
- ☐ The information or record is accurate and complete
- ☐ The patient does not have a right to access the information or record
- ☐ The dental practice did not create the information or record

You have the right to give us a written statement disagreeing with this denial. The statement may not be longer than one page. If you would like to give us a statement, please mail it to our Privacy Official at the address below. If you do not give us a statement of disagreement, you may ask us to give your request for amendment and our denial every time we disclose the information that you wanted us to amend.

If you are concerned that we may have violated your privacy rights, or you disagree with a decision we made about your health information or in response to a request you made, you may file a complaint with our dental office using by contacting our Privacy Official at the address below, or calling our Privacy Official at **<telephone number>**. 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, or you can follow the instructions at on this web page: *http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html*.

If you have any questions about this notice, please contact:

Privacy Official: _____

Address: _____

Telephone Number: _____

Appendix 2.14.2.3

Sample Amendment Request Log

This sample form illustrates how a dental practice might document the practice's responses to patient requests to amend information in a designated record set.

Patient Name	Amendment Requested	Approved or Denied?	If Approved:		
			Date Amendment Completed	List any Third Parties who must be notified of the amendment	Date Amendments Sent to Third Parties

Appendix 2.14.3.1

Sample Log of Disclosures of Patient Information

This sample form illustrates how a dental practice might log disclosures of patient information, so that the practice is prepared in case a patient asks for an accounting of disclosures.

Patient Name	Date of Disclosure	Who received the information?	Description of protected health information disclosed	Purpose of Disclosure	Was the disclosure for research?	Is this one of multiple disclosures that can be grouped?

Appendix 2.14.3.2

Sample Request for Accounting of Disclosures

This sample form illustrates how a dental practice might document a patient's request for an accounting of disclosures of the patient's protected health information.

Notice to Patients: Please use this form to make a request that our practice provide you with an accounting of disclosures of your protected health information.

Patient Name: _____

Disclosure Accounting Request

Time Frame

Please specify the dates between which you would like for our practice to account for disclosures of your protected health information. Under HIPAA, we are not required to include certain disclosures, including disclosures for treatment, payment or healthcare operations.

Starting Date for Disclosure: _____

Ending Date for Disclosure: _____

Our Practice's Contact Person

Please contact _____, our practice's Privacy Official if you have any questions relating to your Accounting of Disclosures request.

Patient Information

Print Name: _____

Signature: _____ Date: _____

Patient's Date of Birth: _____

Appendix 2.14.4

Sample Request for Confidential Communications

This sample form illustrates how a dental practice might document a patient's request that the practice communicate with the patient in a different way or at a different place.

To the Patient: Use this form if you would like our dental practice to communicate with you other than at your primary phone number and/or address. Fill out this request in its entirety.

Patient Name (print): _____

Alternative Communication Request (Please tell us the way you would like us to communicate with you, and/or the address you would like us to use): _____

_____

_____

Payment Information
Your request may affect our normal billing and payment procedure. Please specify any alternative method for handling payment.

_____

_____

Caution: there is some level of risk that third parties might be able to read unencrypted emails.

Patient Signature: _____ Date: _____

For Personal Representatives of the Patient

Print Name of Personal Representative:_____

Relationship to the Patient: _____

Appendix 2.14.5

Sample Request for Restricted Use or Disclosure

This sample form illustrates how a dental practice might document a patient's request for a restriction on the use or disclosure of the patient's information.

Please check and complete either A or B, as applicable.

☐ **A. Health Plan Restriction for items/services paid for in full.**

Patient Name: _____ (please print) asks the dental practice not to give information about the following item(s) and/or service(s), for which the dental practice has been paid in full, to the health plan indicated below, for purposes of payment or health care operations, unless required by law:

Item(s) or service(s): _____

Health plan: _____

*I understand that the dental practice **must agree** to this requested restriction if the practice has received payment in full for these item(s) or service(s).*

Patient Signature: _____ Date: _____

Dental Practice: has payment in full been received? ☐

Dentist or Administrator's Signature:

_____ Date: _____

☐ **B. Other Restriction.**

Patient Name: _____ (please print) asks the dental practice not to use or disclose the information indicated below in the manner indicated below:

Description of information: _____

_____

Requested restricted use and/or disclosure: _____

_____

*I understand that the dental practice **is not required** to agree to this requested restriction, but that if the dental practice does agree it can end the restriction by telling me. I understand that if the dental practice agrees to the restriction, the dental practice may use and disclose the restricted information in certain circumstances, such as for emergency treatment or public health disclosures.*

Patient Signature: _____ Date: _____

Dentist or Administrator's Signature:

_____ Date: _____

For Dental Office Use Only

☐ Agree to

☐ Not Agree to

NOTE: The dental practice **must agree** to a request for disclosure to a health plan of information about a health care item or service for which the dental practice has been paid in full (see Section A of this form).

Signature: _____ Date: _____

Appendix 2.15

Sample HIPAA Training Sign-in Sheet

This sample form illustrates how a dental practice might document that the dental practice's workforce members have received HIPAA training.

Name of Trainer: _____

Trainer's Company Affiliation: _____

Length of Training: _____ Date of Training: _____

Topics Included in Training (attach outline): _____

_____

_____

_____

_____

_____

Attendee List

Print Name	Signature	Date

Appendix 2.22.1
Sample Breach Assessment Form

This sample form illustrates how a dental practice might assess suspected breaches of unsecured protected health information.

A. DESCRIBE THE INCIDENT:

- Date the suspected breach was discovered:
- Date the suspected breach occurred:
- Brief statement of what happened:
- How we learned of the breach:
- Describe the kind of information involved:
- Describe the people and entities involved:
- If the incident involved a *use*[1] of information:
    - Who used the information?
    - For what purpose?
- If the incident involved a *disclosure*[2] of information:
    - Who disclosed the information?
    - To whom?
    - For what purpose?
- Describe the format of the information (e.g., paper records, films, electronic):
- If electronic information was involved:
    - Was the electronic information in storage? (e.g., on a desktop computer hard drive, a laptop, a CD or a USB drive)
    - Was the electronic information in transit? (e.g., in an email or through a portal)
    - Was the electronic information appropriately encrypted?
    - Was the password of an authorized person/entity used to access the information?
- What is being done to mitigate any risk to the privacy and security of the information?

B. IF ANY OF THE FOLLOWING APPLY, HIPAA DOES NOT REQUIRE NOTIFICATION:[3]

1. If the information was properly "secured" using a method approved by the U.S. Department of Health and Human Services ("HHS"):

   Was the information "secured"? ☐ Yes ☐ No
   If yes, explain: _____

   _____

[1] HIPAA defines "use" as the sharing, employment, application, utilization, examination, or analysis of information within an entity that maintains the information.
[2] HIPAA defines "disclosure" as the release, transfer, provision of access to, or divulging any manner of information outside the entity holding the information.
[3] However, other applicable law may apply, such as state or local data security laws.

2. If the information was not "protected health information" ("PHI") as defined by HIPAA.[5]

   Was the information PHI? ☐ Yes ☐ No
   If no, explain:_____

   _____

3. If the use or disclosure was permitted or required under the HIPAA Privacy Rule.

   Was the use or disclosure permitted or required? ☐ Yes ☐ No
   If yes, explain: _____

   _____

4. If the use or disclosure was authorized by the patient in compliance with the HIPAA Privacy Rule.[6]

   Did the patient appropriately authorize the use or disclosure? ☐ Yes ☐ No
   If yes, attach a copy of the signed authorization form.

5. If any of the following exceptions apply:

   Exceptions 1:

   - The incident involved unintentional acquisition, access or use of PHI by a workforce member, or by an individual or entity acting under the authority of the dental practice or one of its business associates,
   - The acquisition, access or use was made:
     - In good faith, and
     - Within the scope of authority, and
   - The acquisition, access or use does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule.

   Exception 2:

   - The incident involved an inadvertent disclosure:
     - by an individual or entity that is authorized to access PHI at the dental practice (or one of its business associates),
     - to another person authorized to access PHI at the dental practice (or the same business associate), and
   - The information received as a result of such disclosure was not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule.

[5] Information, including demographic and genetic information, is PHI if it:
- Is in any format, including oral, electronic, or hard copy (e.g., paper, film or photograph),
- Was created or received by a health care provider, health plan, employer, or health care clearinghouse,
- Relates to:
  - the past, present, or future physical or mental health or condition of an individual,
  - the provision of health care to an individual, or
  - the past, present, or future payment for the provision of health care to an individual, and
  - Includes one of the 18 HIPAA identifiers (see Chapter 2, Section 2.2.8 of *The ADA Practical Guide to HIPAA Compliance Privacy and Security Manual*), or if there is a reasonable basis to believe the information can be used to identify the individual, unless
- The information is:
  - Employment records held by the dental practice in its role as an employer
  - Education records covered by the Family Educational Rights and Privacy Act ("FERPA")
  - Information regarding an individual who has been deceased for more than 50 years.

[6] See "Authorization," Section 2.2.7, Chapter 2, of *The ADA Practical Guide to HIPAA Compliance Privacy and Security Manual.*

Exception 3:

- The incident involved a disclosure of PHI, and
- The dental practice or business associate (as applicable) has a good faith believe that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Does one of the three above exceptions apply? ☐ Yes ☐ No
If yes, explain: _____

_____

C. RISK ASSESSMENT:

If the information was unsecured PHI, and

- the use or disclosure was not permitted or required under HIPAA,
- the individual did not appropriately authorize the use or disclosure, and
- none of the exceptions above apply,

then the dental practice must send timely breach notification unless the dental practice demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of the relevant factors, including at least the following factors:

Factor 1: The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.

Assessment:

Factor 2: The unauthorized person who used the protected health information or to whom the disclosure was made.

Assessment:

Factor 3: Whether the PHI was actually acquired or viewed.

Assessment:

Factor 4: The extent to which the risk to the PHI has been mitigated.

Assessment:

Should any additional relevant factors be considered in determining the probability that the PHI has been compromised? If so, describe:

_____

_____

Assessment:

Based on a risk assessment involving all of the above factors, is there an overall low probability that the PHI has been compromised?

- **The probability of compromise is LOW:** _____
- **The probability of compromise is NOT LOW:** _____

IF THE PROBABILITY THAT PHI HAS BEEN COMPROMISED IS NOT LOW, HIPAA BREACH NOTIFICATION IS REQUIRED.

Is notification required under other applicable federal, state or local law? ☐ **Yes** ☐ **No**

If yes, explain: _____

_____

_____

This risk assessment form is accurate and complete.

Signed: _____

Name: _____

Title: _____ Date:_____

Appendix 2.22.2

Sample Breach Log

This sample form illustrates how a dental practice might log breaches that affect less than 500 individuals for annual submission to the U.S. Department of Health and Human Services. The following information must be recorded for every breach of unsecured patient information.

Date of breach: _____

Date breach was discovered:_____

Did the breach occur at or by a business associate?

- ☐ Yes
- ☐ No

If yes:

Name of business associate: _____

Address: _____

City:_____ State: _____ Zip code: _____

Business associate contact name:_____

Business associate contact phone number:_____

Business associate contact email:_____

Approximate number of individuals affected by the breach: _____

Type of breach:

- ☐ Theft
- ☐ Loss
- ☐ Improper disposal
- ☐ Unauthorized access or disclosure
- ☐ Hacking or information technology incident
- ☐ Unknown
- ☐ Other: _____

Where was the breached information located?

- ☐ Laptop
- ☐ Desktop computer
- ☐ Network server
- ☐ Email
- ☐ Other portable electronic device
- ☐ Other
- ☐ Electronic medical record
- ☐ Paper

Type of patient information involved:

- ☐ Demographic information
  - o Name
  - o Social Security number
  - o Address or zip code
  - o Driver's license number
  - o Date of birth
  - o Other identifier
- ☐ Financial information
  - o Credit card or bank account number
  - o Claims information
  - o Other financial information
- ☐ Clinical information
  - o Diagnosis or conditions
  - o Lab results
  - o Medications
  - o Other treatment information
- ☐ Other

Brief Description of the breach (include the location of the breach, a description of how the breach occurred, and any additional information regarding the type of breach, type of media, and type of protected health information involved in the breach):

_____

_____

_____

What safeguards (protective measures) were in place prior to the breach:

- ☐ Firewalls
- ☐ Packet filtering (router-based)
- ☐ Secure browser sessions
- ☐ Strong authentication
- ☐ Encrypted wireless
- ☐ Physical security
- ☐ Logical access control
- ☐ Anti-virus software
- ☐ Intrusion detection
- ☐ Biometrics

Date(s) notice was provided to affected individual(s):

Date first notice was sent:

Month: _____ Day: _____ Year: _____

Date last notice sent:

Month: _____ Day: _____ Year: _____

Was substitute notice required? (Substitute notice is required if you lack sufficient or up-to-date contact information for any affected individuals)

☐ Yes

☐ No

Was media notice required? (Media notice is required if a breach involves 501 or more residents of a state or jurisdiction)

☐ Yes

☐ No

What action did the dental practice take in response to the breach?

☐ Security and/or privacy safeguards

☐ Mitigation (actions to lessen the harm of the breach to affected individuals)

☐ Sanctions (against workforce members who violated the policies and procedures)

☐ Policies and procedures

☐ Other

If "other," please describe: _____

Describe in detail any additional actions taken following the breach:

_____

_____

_____

_____

This form provides for the recording of the information required by the Office for Civil Rights ("OCR") when submitting reports of breaches. See OCR, *Notice to the Secretary of HHS of Breach of Unsecured Protected Health Information http://ocrnotifications.hhs.gov.* **This material is for general reference purposes only and does not constitute legal advice. It covers only HIPAA, not other federal nor state law. Changes in applicable laws or regulations may require revision. Dentists should contact qualified legal counsel for legal advice, including advice pertaining to HIPAA compliance, the HITECH Act, and the U.S. Department of Health and Human Services rules and regulations.**

Appendix 2.22.3

Sample Agreement to Receive Electronic Communication

This sample form illustrates how a dental practice might obtain patient agreement to receive communications via email.

Patient Name: _____ Date of Birth: _____

I agree that the dental practice may communicate with me electronically at the email address below.

I am aware that there is some level of risk that third parties might be able to read unencrypted emails.

I am responsible for providing the dental practice any updates to my email address.

I can withdraw my consent to electronic communications by calling:

_____**[practice's telephone number]**.

Email Address (PLEASE PRINT CLEARLY):

_____@_____

Patient Signature: _____ Date:_____

Appendix 2.22.4
Full Disk Encryption Q&A

INTRODUCTION

Why encrypt?
When electronic patient information is properly encrypted, HIPAA does not require breach notification even if the device that stores the information is lost or stolen, as long as the encryption key (e.g., the password) is not compromised. For example, if a covered dental practice stores patient information on a laptop computer and the laptop is stolen, the dental practice does not need to send breach notification if the dental practice can demonstrate that the laptop is properly encrypted and the encryption key is secure.

How to encrypt?
A variety of methods can be used to encrypt data "at rest" (i.e., stored data) or data "in transit" (such as an email). **This resource only discusses encrypting data at rest using the method known as "full disk encryption" ("FDE")**. A variety of FDE products are available. Several products are discussed below as examples only.

Are there risks to using FDE?
Yes. Remembering your password is crucial when your computer is protected with FDE. ***If you forget your password you may not be able to recover your data!*** Securely backing up your data may also help with recovery (see below). Whether or not you back up your data, it is important to ***protect your password.*** If both a properly encrypted computer and the password are stolen, HIPAA may require breach notification even though proper encryption was used.

What is "Full Disk Encryption" (or FDE)?
- It is a security tool that unobtrusively encrypts your entire computer hard drive
- This encryption secures your hard drive so that no one can access it without a valid password.
- This tool becomes important to you if your computer is lost or stolen.

The password you already use to log onto your computer isn't enough. Why not?
- Password protection alone does not "secure" patient information under the HIPAA Breach Notification Rule.
- Unfortunately, Windows and Macintosh passwords offer only limited protection of your data. If a computer protected only with a password is stolen, HIPAA may require sending breach notification.
- Even though your computer is protected by a password, it is still relatively easy for someone to access your data. They don't need to know your password to do so. They only need physical access to your computer and a little bit of technical knowledge.
- One way is to boot another operating system from your CD-ROM drive or from a USB drive. For example, a person who has your computer can boot a copy of Linux from CD-ROM and then access your Windows or Macintosh hard drive the same way you would access any USB drive.
- Another way is to remove your hard drive from your computer and temporarily attach it to another computer, again sort of like a USB drive.
- In either case, any file on your computer could be accessed without your permission or knowledge, if someone had possession of your computer.

Using "Full Disk Encryption" is a simple way to prevent someone who steals your computer from accessing any patient information on the computer.

How Full Disk Encryption works
- You first obtain Full Disk Encryption software and install it.
- The software uses a password that you provide to encrypt your entire computer's hard drive.
- When you start up your computer, you may be prompted for a boot up password (this is an option for some software). If not, you will be prompted for your usual login password (which should also be a strong password — see "Strong Passwords" below).
- If a person tries to boot another operating system and access your files, they will not be able to see any data because they do not have the encryption password.
- If a person removes your hard drive and tries to access the files, they will not be able to see any data because they do not have the encryption password.

- In order to access a hard drive that has been encrypted using Full Disk Encryption, you need to know either the encryption password or a valid login password, depending on the configuration.

Where can I obtain Full Disk Encryption software?

There are any number of appropriate products available, but here are a few examples:

- If you're using the Pro Enterprise editions of Windows 8 or later, or Windows 7 Ultimate or Enterprise, or Vista Ultimate or Enterprise, you can enable the built in Bitlocker software, which provides Full Disk Encryption.
- If you're a Macintosh user, the versions of Apple's OS X called "Yosemite" and "El Capitan" include an enhanced version of a tool called FileVault. FileVault includes Full Disk Encryption functionality. OS X Yosemite was released in October 2014 and El Capitan was released in June 2015.
- Another product available for either Windows or Macintosh computers is Symantec's PGP Whole Disk Encryption. This software costs about $100 per computer.

If you wish to use FDE software, make sure that the FDE software complies with one of these standards:

- It is FIPS 140-2 (Federal Information Processing Standards) validated. We are unaware of any FDE software that is not FIPS 140-2 validated, but you should verify.
- Alternately, confirm that your FDE software uses AES encryption with 128 bit keys or longer.

After you've installed Full Disk Encryption:

- Don't forget your FDE password. If you do, you may lose data.
- Do regular backups of the computer protected with FDE. This is a good idea under any circumstances, but if you have a hard drive failure, it may be impossible for a hard drive recovery service to recover your data files even though you've provided the FDE password.
- When you perform those backups, be sure to encrypt them using a strong password and AES 128 bit encryption at a minimum.

If you previously encrypted your computer using TrueCrypt, you should investigate other FDE products. TrueCrypt was discontinued in May of 2014, and support is no longer available. Therefore, this software is no longer a source for FDE.

If the application you're using to store patient information (such as a Dental Practice Management system) encrypts that data within the application, FDE may not be required to avoid breach notification in the event of the theft or loss of a computer. However, using FDE in this situation provides a second level of security.

Strong Passwords

A strong password is not easy to guess. Suggestions for constructing a strong password:

- Make the password at least eight characters long (ten or twelve is even better)
- Use upper and lower case letters, numerals, and punctuation symbols
- Do not use:
  - Words that can be found in a dictionary (English or foreign language) or words from fictional languages, names of famous people, famous fictional characters, and so forth
  - Words that are part of your name
  - Doubling up of words (such as "golfgolf")
  - Patterns such as "12345678," "qwerty," "asdfgh," etc.
  - Prefixing or suffixing any word found in sources listed above with numbers (for example, "1password" or "password1")
  - A commonly used sentence or song lyric, such as "To be or not to be," or "Oh say can you see."

Changing passwords regularly, and never reusing old passwords, helps protect data.

Data can be compromised if an unauthorized person obtains or guesses a password — for example, if a password is easy to guess or is not a "strong password," if someone posts a password on a computer or stores it in a laptop case, or if someone stores passwords electronically in an unencrypted Microsoft Word document.

Appendix 2.23
Sample Complaint Log

This sample form illustrates how a dental practice might log complaints about the dental practice's privacy practices or HIPAA compliance.

Complaint	Name and contact information of the person making the complaint	Date complaint was made	Date response sent to person who made the complaint	Sanctions, if any	Describe any changes resulting from the complaint i.e. training, process redesign