Dr. Michael J. Goulding DDS

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, counter-intelligence and other national security activities. We may disclose protected health information to a correctional insititution or an enforcement official having lawful custody of an inmate or patient.

Appointment Reminders: We may use or disclose your health information to provide you with appointment reminders (voicemail messages, e-mails or text messages).

Patient Rights: You have the right to view or attain copies of your health information with limited exception. You must make a request in writing to obtain access to your health information. A form requesting access may be obtained by utilizing the contact information at the endo of this notice.
We have the right to charge a reasonable cost for expenses based on the difficulty of the task. If you request *additional* copies of your records made, a rate of $1.00 per page or $25.00 per hour will be charged (for locating the record and proper duplication of information), plus postage should you require that these copies be mailed to you. You may request that we provide copies in a format other than photocopies. We will use the format you request, unless we cannot practically do so.
If full records are not required, we can prepare a summary of your health information.

Disclosure Accounting: You have the right to receive a list of instances in which we or out business associates disclosed your health information for purposes other than treatment, payment or healthcare operations for any time in the last 6 years, but not before April 14, 2003. If you request this accounting more than once in a twelve-month period, a reasonable cost will be charged for responding to these additional requests.

Restriction: You have the right to request that we place additional restrictions on our use or disclosure of your health information. We are not required to agree to any additional restrictions, but will abide by any which we *do*. In the case of a medical emergency, these additional restrictions may be ignored if it is felt that by following them, your well-being would be placed in jeopardy.

Alternative Communication: You have the right to request us to communicate with you by alternative methods or in other locations. These requests must specify these changes and make your request in writing. Such requests, if they are agreed upon, may incur additional expenses for travelling etc.

Amendment: You have the right to request that we amend your health information. (This request must be in writing and satisfactorily explain the reason for amendment.) Under certain circumstances, we may deny this request.

Electronic Notices: If you receive this notice on our website or by electronic mail (e-mail), you are entitled to receive this notice in written form.

Questions and Complaints: If you require more information about our privacy practices, have questions or concerns or wish to amend, restrict or acquire of copy of your records please contact us.
If you are concerned that we may have violated your privacy rights or you disagree with a decision made regarding access to your healthcare information, you may complain using the contact information listed at the end of this notice. You may also submit a written complaint to the U.S. Department of Health and Human Services.

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 either with us or with the U.S. Department of Health and Human Services.

To Contact Office:
Michael J. Goulding DDS
Address: 3600 Hulen St. Suite A-3
Fort Worth, TX 76107
Telephone: 817-737-3536
Fax: 817-737-3689

Addendum to the Health Insurance Portability and Accountability Act (HIPAA) Omnibus

The federal government has published its final regulations implementing the "Health Information Technology for Economic and Clinical Health (HITECH) Act," enacted as part of the "American Recovery and Reinvestment Act of 2009" (ARRA), which in turn changes the HIPAA Privacy and Security rules. The new rules expand the obligations of physicians and other health care providers to protect patients' Protected Health Information (PHI), extend those obligations to a host of other individuals and companies, who, as "business associates," have access to PHI, and increase the penalties for violations of any of these obligations. Changes to existing policy to meet with new HIPAA requirements is required by September 23, 2013, the compliance date.

Privacy and Security Policies and Procedures

The obligation to notify patients if there is a breach of their PHI is a breach of their PHI is expanded. Breaches now are presumed reportable unless, after completing a risk analysis, it is determined, that there is a "low probability of PHI compromise." The doctors must consider *all* of the following four factors:
--the nature nd extent of the PHI involved--issues to be considered include the sensitivity of the information and the likelihood the information can be re-identified;
--the person who obtained the unauthorized access and whether that person has an independent obligations to protect the confidentiality of the information;
--whether the PHI was actually acquired pr accessed, determined after conducting a forensic analysis; and
--the extent to which the risk has been mitigated, such as by obtaining a signed confidentiality agreement from the recipient.

This rebuttal presumption of breach and four factor assessment of the "risk of PHI compromise" replaces the previous, more subjective "significant risk of financial, reputational, or other harm" analysis for establishing a breach. The new rules further clarify that there is no need to have an independent entity conduct the risk assessment and indeed, no risk assessment need be conducted at all if the breach notification is made. The new rules further confirm that the breach notification requirement may be delegated to a BA.

Disclosures to health plans--At the patient's request, physicians may not disclose information about care the patient has paid for out-of-pocket to health plans, unless for treatment purposes or in the rare event the disclosure is required by law. The new law requires health care providers to abide by a patient's request not to disclose PHI to a health plan for those services for which the patient has paid out-of-pocket and requests the restriction

Marketing Communications--The new rules further limit the circumstances when doctors may provide marketing communications to their patients in the absence of the patient's written authorization. The only time a health care provider may tell a patient about a third-party's product or service without the patient's written authorization is when: 1) no compensation is received for the communication; 2) the communication is face-to-face; 3)the communication involvesa drug or biologic the patient is currently being prescribed and the payment is limited to reasonable reimbursement of the costs of the communication (no profit); 4) the communication involves general health promotion, rather than the promotion of a specific product or service; or 5) the communication involves government or government-sponsored programs. Healthcare providers are still permitted to give patients promotional gifts of nominal value (e.g. pamphlets and product samples).

Sale of PHI--The prohibition on the sale of PHI in the absence of the patient's written authorization extends to licenses or lease agreements, and to the receipt of financial or in-kind benefits. It also in-

cludes disclosures in conjunction with research. The prohibition on PHI sales does not extend to permitted disclosures for payment or treatment nor to permitted disclosures.

Decedents--The new rules allow physicians to make relevant disclosures to the deceased's family and friends under essentially the same circumstances such disclosures were permitted when the patient was alive. The new rule also eliminates any HIPAA protection for PHI 50 years after a patient's death.

Copies of e-PHI--Doctors will now have only 30 days to respond to a patient's written request for his or her PHI with one 30 day extension. They must provide access to EHR and other electronic records in the electronic form and format requested by the individual if the records are "readily reproducible" in that format. Otherwise, they must provide the records in another mutually agreeable electronic format. Hard copies are permitted only when the individual rejects all readily reproducible e-formats.

E-mailing PHI--Physicians must also consider transmission security, and may send PHI in unencrypted e-mails only if the requesting individual is advised of the risk and still requests that form of transmission.

Charging for copies of e-PHI or PHI--The new rules modify the costs that may be charged to the individual for copies to include labor costs, paper, postage, the cost of any portable media (such as a USB memory stick or CD), assuming state law does not set a lower reimbersement rate. The rules also clarify that health care providers may impose a separate charge for creating an affidavit of completeness.

Notice of Privacy Practices (NPP)

Health care providers must amend their NPPs to reflect the changes set forth above, including those related to breach notification, disclosures to health plans, and marketing and sale of PHI. To the extent doctors engage in fundraising, they will also have to amend their NPP to inform patients of their right to opt-out of those communications. Doctors will need to post the revised NPP and make copies available at their office, to all new patients and to anyone else on request. Healt care providers who maintain a website must post the updated NPP on their website as required by the existing HIPAA privacy rule.

Business Associates (BAs)

These rules modify the requirements for BA agreements:

--Doctors no longer must report failures of their BAs to the government when termination of the agreement is not feasible, as HHS has concluded that the BA's direct liability for these violations is sufficient.

--BAs are now responsible for their subcontractors.

--BAs must comply with the Security and Breach Notification Rules.

--Doctors are liable for the actions of their BAs who are agents, but not for the actions of those BAs that are independent contractors.

BA agreements that have not been renewed or modified between March 26, 2013 and September 23, 2013 will be deemed compliant until the date the BA agreement is renewed or modified or until September 22, 2014, whichever is earlier.

Enforcement and Penalties

The new rules clarify the four penalty tiers as follows:

--Lowest tier- cases in which the physician did not and reasonable could not know of the breach.

--Intermediate tier- cases in which the physician "knew, or by exercising reasonable diligence would have known" of the violation, but the physician did not act with willful neglect.

--Highest tiers- cases in which the physician "acted with willful neglect" and either corrected the problem within the 30-day cure period, or failed to make a timely correction.

The assessment of penalties must be based on five principle factors: (1) the nature and extent of the violation, including the number of individuals affected; (2) the nature and extent of the harm resulting from the violation, including reputational harm; (3) the history and extent of prior compliance; (4) the financial condition of the covered entitiy or business associate; and (5) such other matters as justice may require. The number of violations may be based on the number of individuals affected or by the number of days of non-compliance.

The rule further clarifies that the 30-day cure period begins when the physician knew or should have known of the violation.

Other Changes

The new rules also implement the Genetic Information Nondiscrimination Act (GINA), which generally prohibits health plans from using genetic information for underwriting purposes.