Neal, Gerber & Eisenberg LLP

HEALTH LAW CLIENT UPDATE
March 2004

Are You Compliant?

Next Phase of HIPAA Compliance Dates Starts April 14, 2004

INFORMATION PRIVACY

The Compliance Date for Small Health Plans Is Almost Here. Small health plans must comply with the Privacy Rule starting April 14, 2004. After April 14, the only health plans that will not be subject to the Privacy Rule are group health plans that have less than 50 participants *and* that are administered *solely* by their employer-sponsors. The Privacy Rule applies to all other group heath plans (the "covered group health plans").

What is a small health plan? A health plan, including a covered group health plan, that had annual receipts of not more than $5 million for its fiscal year ending before April 14, 2003 is a small health plan with an April 14, 2004 Privacy Rule compliance date. The annual receipts of a group health plan are the combination of premiums paid for any insured benefits and claims paid for any self-funded benefits.

What must a small health plan do to comply with the Privacy Rule? It must (a) implement written privacy policies and procedures, (b) distribute a notice of privacy practices, (c) appoint a privacy official and designate a contact office, (d) train workforce members on its privacy policies and procedures and sanction those who violate them, (e) obtain compliant written contracts with business associates, (f) provide individuals with access to, amendment of, and an accounting for certain disclosures of protected health information, (g) have a privacy complaint procedure, (h) implement reasonable administrative, physical and technical safeguards for protected health information, and much more. It may not use or disclose protected health information except as the Privacy Rule permits or requires.

Do these compliance obligations apply to covered group health plans? Yes. Every covered group health plan that is self-funded in part or whole or that creates or receives protected health information beyond enrollment data and summary health information (which is essentially aggregated claims data without individual identifiers) must comply fully with the Privacy Rule.

On the other hand, a group health plan that provides health benefits *solely* through insurance contracts and that creates or receives no more than enrollment data and summary health information must comply with the Privacy Rule, but has significantly reduced administrative compliance requirements.

How does the Privacy Rule impact an employer's access to plan enrollees' information? Unlike the covered group health plans they sponsor, employers are not subject to the Privacy Rule. The Privacy Rule nonetheless impacts employers' relationships with their group health plans and with the administrators and insurers of the plan's benefits.

The Privacy Rule restricts the information about plan enrollees that may be disclosed to an employer. The Privacy Rule allows a group health plan and its administrator or insurer to disclose enrollment data to the employer and summary health information if the employer requests it to obtain premium bids for health insurance coverage or to modify, amend, or terminate the plan.

What if the employer wants to be involved in plan administration? An employer that wants other kinds of protected health information so it may perform plan administration functions must amend the plan document to promise to safeguard protected health information. These safeguards must include the employer's promise never to use protected health information for any employment-related action or decision or for any other benefit or benefit plan.

The Grace Period for Obtaining Compliant Business Associate Contracts Is Almost Over. The grace period for obtaining compliant business associate contracts ends on April 14, 2004. The grace period was available for business associate relationships existing before October 15, 2002 that are evidenced by a writing that did not expire and was not renewed before April 14, 2004.

ELECTRONIC TRANSACTIONS

Starting July 1, Medicare Will Slow Payments on Non-Compliant Electronic Claims. Medicare will slow payment of electronic claims that do not comply with the Transactions Rule claims standard. Medicare currently pays electronic claims within 14 days, but after July 1, electronic claims must be in the ASC X12N 837 standard format to receive such prompt payment.[1] Non-compliant electronic claims will take as long as paper claims—27 days.

Most Providers Must Submit Electronic Claims to Be Paid by Medicare. Once CMS terminates its "contingency plan," under which it continues to accept claims that are not HIPAA-compliant, providers (other than "small providers") will have to submit claims to Medicare electronically to be paid. The "small providers" allowed to submit paper claims are physicians, practitioners, facilities, and suppliers with less than 10 full-time equivalent employees, and hospitals, skilled nursing facilities, home health agencies, hospices, and similar providers of services with less than 25 full-time equivalent employees. CMS has yet to indicate when it will end its "contingency plan."

DATA SECURITY

The Compliance Date Is Only a Year Away. Health plans (other than small health plans), health care providers who transmit or have transmitted on their behalf electronic transactions regulated by the Transactions Rule,[2] and health care clearinghouses will have to comply with the HIPAA Security Rule starting April 20, 2005. The Security Rule compliance date for small health plans is April 20, 2006.

What does the Security Rule require? The Security Rule requires a comprehensive assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by a covered entity, and the implementation of a variety of administrative, physical, and technical safeguards, based on that assessment, that will reduce those risks and vulnerabilities to a reasonable and appropriate level.

Will the Security Rule affect business associate relationships? Yes. The Security Rule mandates that specified safeguards be added to business associate contracts involving electronic protected health information. It is not too early to begin adding these terms to business associate contracts.

Will the Security Rule affect employers sponsoring group health plans? Yes. The Security Rule mandates specified safeguards be added to the plan document amendment required before an employer may receive electronic protected health information to perform administration functions for the group health plan it sponsors.

NATIONAL PROVIDER IDENTIFIER

The National Provider Identifier Rule Has Been Issued. The final rule for the "national provider identifier" or "NPI" was issued on January 23, 2004. Health care providers may begin obtaining NPIs on May 23, 2005. There will be no fee for an NPI.

What is the NPI? The NPI is a 10-digit numeric identifier with no intelligence about the health care provider to whom it is assigned. Each NPI will be uniquely associated with a single health care provider. An issued NPI will not be reused or reassigned. A provider's NPI will never change (unless unusual circumstances, such as fraudulent use by another, justify its replacement).

[1] Retail pharmacy drug claims must be submitted in the NCPDP Telecommunication Standard Version 5.1 format.

[2] The Transactions Rule currently regulates eight transactions: (1) health care claims; (2) health care remittance advice; (3) health care claim status; (4) eligibility for a health plan; (5) referral certification and authorization; (6) coordination of benefits; (7) enrollment and disenrollment in a health plan; and (8) health plan premium payments.

What are the compliance dates? Providers subject to HIPAA, health plans that are not small health plans, and health care clearinghouses must begin using NPIs in standard transactions on May 23, 2007. Small health plans will not be required to use NPIs in standard transactions until May 23, 2008.

Who must get an NPI? Every provider who transmits electronically, or has transmitted electronically on its behalf, transactions regulated by the Transactions Rule *must* obtain an NPI no later than May 23, 2007. These are the "covered health care providers."

An individual who is a provider and who conducts his or her own electronic transactions regulated by the Transactions Rule is a covered health care provider who must have an NPI, even if employed by an organizational health care provider, such as a hospital, clinic, or group practice.

A covered organizational health care provider must obtain an NPI. It may elect to get (a) one NPI for the entire organization, (b) an NPI for each one of its subparts that would be a covered health care provider if it were a separate legal entity, or (c) an NPI for itself and for any one or more of its subparts, including subparts that would not qualify as covered health care providers if they were separate legal entities. A subpart is any unit of the organization that can be uniquely identified, for example, by separate physical location, by separate license or certification, or by separate billing, from the organization of which it is a part.

May other providers get NPIs? Yes. A provider not subject to HIPAA may elect to obtain an NPI. Having an NPI will *not* subject the provider to HIPAA. Transmitting an electronic transaction regulated by the Transactions Rule will.

How will NPIs be used? Covered entities must use only the NPI in standard transactions that require an NPI to identify a provider. Covered entities must require their business associates to use NPIs as required by any standard transaction that the business associates conduct on their behalf.

NPIs may be used for any other lawful purpose. For example, NPIs may be used to identify providers in medical records, for debt collection, and to cross-reference fraud and abuse and program integrity files.

How will covered entities find out what a provider's NPI is? To ensure that NPIs will be available for standard transactions, covered health care providers must disclose their NPIs upon request to anyone needing the NPIs for standard transactions. Health plans and others needing NPIs for standard transactions will also be able to obtain providers' NPIs from the National Provider System, which will manage NPI issuance and maintenance.

EMPLOYER IDENTIFIER

The Compliance Date Is Approaching. The compliance date for use of the employer identifier in standard transactions is July 30, 2004 for all covered entities except small health plans. The compliance date for small health plans is August 1, 2005.

What is the employer identifier? The employer identifier is the employer identification number or "EIN" issued by the Internal Revenue Service.

How will the EIN be used? The EIN will be used in standard transactions to identify an employer acting as an employer. It does not identify a group health plan that the employer sponsors.

The standard transactions that use the EIN are generally limited to those involving employers and health plans. Because employers are not subject to HIPAA, employers are not required to conduct standard transactions. If an employer decides to do so, however, a health plan which has a business relationship with that employer must accept the employer's standard transaction.

HIPAA ENFORCEMENT

The Enforcement Procedure Rule Sunsets September 16, 2004. The interim rule setting the procedures for civil HIPAA enforcement by the Department of Health and Human ("DHHS") will expire on September 16, 2004. DHHS intends to issue a complete enforcement rule addressing both procedural and substantive requirements, but has not yet proposed such a rule.

Statutory Sanctions for HIPAA Violations Are In Effect. HIPAA makes it a federal crime to knowingly misuse or cause to be misused a unique health identifier, such as the NPI, and to knowingly obtain or disclose individually identifiable health information in violation of HIPAA or its implementing regulations.

* * * * *

Our Health Law Group includes nationally recognized experts on HIPAA compliance. For information, please contact Jack Rovner (312-269-8014, jrovner@ngelaw.com), Kathy Roe (312-269-8043, kroe@ngelaw.com), Tom Bixby (312-269-8050, tbixby@ngelaw.com), or Micki Unkrich (312-269-5233, munkrich@ngelaw.com).

HEALTH LAW PRACTICE GROUP

The Health Law Group at Neal, Gerber & Eisenberg LLP advises and assists health care organizations with effective management of the ever-changing challenges of the business of health care. We provide strategic counseling, compliance and transactional support, and litigation representation for health insurers, managed care organizations, hospitals, integrated delivery systems, long term care providers, professional associations, practitioners, and other health care industry participants. Our strength lies in the quality, innovative solutions we develop with our health care clients to facilitate their strategies and accomplish their goals. For more information or to discuss how we may be able to serve your needs, please contact Dan J. Hofmeister, Jr. (312-269-5310, dhofmeister@ngelaw.com) or Jack Rovner (312-269-8014, jrovner@ngelaw.com), the co-chairs of our Health Law Group.

Neal, Gerber & Eisenberg LLP
Two North LaSalle Street, Chicago, Illinois 60602
(312) 269-8000
www.ngelaw.com

Please note: This publication should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The contents of this publication are intended solely for general purposes. Please consult a lawyer concerning your own situation and any specific legal questions you may have.