NADA MANAGEMENT EDUCATION

NADA MANAGEMENT SERIES® MBULLETIN

Route to:

☐ _____

☐ _____

File under Legal, L.45

HIPAA: Dealership Compliance with the Medical Information Privacy Rule

I. Introduction

The Medical Information Privacy Rule (Privacy Rule) issued by the U.S. Department of Health and Human Services (HHS) implements the Health Insurance Portability and Accountability Act (HIPAA). The Privacy Rule sets standards governing the use or disclosure of individually identifiable health information–referred to as *protected health information*–to help prevent it from being misused in employment decisions and to protect the privacy rights of individual participants in health plans subject to the Rule. HHS has the authority to enforce the Privacy Rule, primarily by responding to complaints. Violations potentially are subject to both civil and criminal penalties.

To understand how the Privacy Rule applies, dealerships must:

- Determine if they sponsor fully-insured or self-funded health plans;
- Find out which dealership employees (if any) handle protected health information;
- Recognize how and when those employees use, disclose, or request protected health information.

II. Protected Health Information (PHI)

Protected health information, or PHI, is health information maintained or received in any form by an entity subject to the Privacy Rule–known as a *covered entity*–that relates to an individual's medical care and is or could be identified with that individual. PHI includes information related to an individual involving:

- the person's past, present, or future physical or mental health or condition;
- the person's health care; or
- past, present or future payments for the provision of the person's health care.

PHI does not include employment records such as certain pre-employment drug tests and physicals, sick leave requests, fitness-for-duty exams, and Family and Medical Leave Act or Americans With Disabilities Act compliance paperwork.

PHI must be disclosed, upon request, to the individual (or authorized representative of the individual) whose information it is, and to HHS during a compliance review or enforcement action. There are numerous circumstances where PHI may be used or disclosed. When in doubt, a written authorization should be obtained from the individual whose information is to be used or disclosed.

PHI may include *summary health information* that has been "de-identified," i.e., cleansed of individually identifiable health information. Summary health information, or SHI, should be used only to modify or terminate plans or to seek new plan or coverage bids. SHI summarizes the claims history, expenses, or types of claims experiences of individuals, and excludes:

- Names;
- Addresses (except state and 5-digit zip code);
- Date and age-related information;
- Phone and fax numbers, E-mail addresses;
- Social security, medical record, health plan beneficiary, account, and certificate/license numbers;
- Vehicle and device identifiers, including serial numbers;
- Web URLs and IP addresses;
- Biometric identifiers;
- Full-face photographs and comparable images;
- Any other unique identifying numbers, characteristics, or codes.

Examples of dealerships handling PHI include human resources personnel who assist plan participants with health claim status questions, final claims arbitrations for self-funded plans, reviews of Third Party Administrator claims handling practices, and health plan administration. Most dealerships handle (or should handle) little, if any, PHI.

III. When Must Dealerships Comply With the Privacy Rule?

Under the Privacy Rule, employers are not regulated. However, regulated covered entities include health plans sponsored or funded by employers. The exact compliance requirements that a plan or plan sponsor must meet depend on the plan's structure, the types of PHI it receives, and the type of PHI it shares with others. Health plans subject to the Rule include group health plans, health insurance issuers, and HMOs providing medical, dental and/or vision coverage, flexible spending accounts, and employee assistance plans. Life, accident, liability, disability, credit, and workers' compensation plans are not considered health plans and are not covered by the Privacy Rule.

Most dealership-sponsored or funded health plans are small health plans (defined as having $5,000,000 or less in annual receipts[1]), and must comply with the Privacy Rule by April 14, 2004. (Large health plans should have complied by April 14, 2003.) Self-administered, self-insured health plans with 50 or fewer participants are exempt from Privacy Rule compliance, but dealerships rarely, if ever, administer their own plans.

A. Dealerships Sponsoring Fully-Insured Plans

Most dealerships sponsor fully-insured health plans. The plans typically have extensive compliance obligations under the Privacy Rule, but sponsoring dealerships need not. Dealerships sponsoring plans that receive no PHI have no compliance obligations. Also essentially exempt from compliance are dealerships sponsoring plans that agree to receive only enrollment and disenrollment (withdrawal) information, PHI for the performance of administrative functions, and/or SHI for purposes of plan modification or termination or to seek bids on new plans or coverage.

Dealerships sponsoring fully-insured plans should avoid handling PHI or SHI except for the limited purposes just noted. In the alternative, they must amend their plan documents and certify compliance with appropriate Privacy Rule requirements.[2] Moreover, dealerships sponsoring fully-insured plans should attempt to direct employees with questions about claims or coverage to appropriate insurance company contacts. ***Dealerships unable to minimize their handling of PHI so as to be effectively exempt from compliance should contact competent counsel for the development of compliance policies, procedures, programs, and documents tailored to their operations.***

B. Dealership Self-Insured Health Plans

Dealerships sponsoring partially or fully self-insured (funded) health plans essentially are considered to be health plans under the Privacy Rule. Those dealerships may even have employees who administer health benefits on behalf of the dealership. Dealership health plans should limit the handling of PHI in order to minimize their Privacy Rule compliance responsibilities.

To the extent that dealership-insured health plans provide health benefits solely through insurance contracts with health insurance issuers or HMOs, and only receive or create SHI or information on whether individuals are participating or are enrolled/disenrolled from the issuer or HMO, they need only refrain from:

- Interfering with employees exercising their rights under the Privacy Rule;
- Requiring persons to waive rights under the Privacy Rule as a condition of receiving payments, enrolling in a plan, or being eligible for benefits.

Furthermore, these plans do not have to meet the compliance requirements (see section IV), or amend health plan documents before sharing information with the dealership sponsor, if the plan or its health insurance issuer or HMO only discloses:

- SHI requested for obtaining premium bids for providing coverage under the plan or for plan modification, amendment, or termination;
- Information on whether individuals are participating in the plan or have enrolled/disenrolled from a plan health insurance issuer or HMO.

Such plans need not provide privacy notices as they will be provided by insurers and HMOs.

Dealership health plans that do not meet the above restrictions (i.e., that use, disclose or receive additional PHI) must issue privacy notices, follow use and disclosure requirements, institute adminis-

trative safeguards, and ensure that individual privacy rights are protected.

As with dealerships sponsoring fully-insured plans, to the extent that dealership-funded health plans cannot minimize the use, disclosure, and receipt of PHI so as to qualify for the compliance exemptions, they should contact competent counsel to assist with compliance responsibilities.

IV. Dealership Health Plan Compliance

Unless a dealership health plan is fully-insured and receives only SHI, it is a covered entity that must comply with the Privacy Rule. The Rule is flexible, allowing dealership health plans with limited access to and interaction with PHI to put relatively simple policies and procedures in place.

A written policies and procedures document must be kept on file. An effective PHI policy and procedures document should contain:

- A statement of purpose;
- A definition of what the policy covers;
- Definitions of key terms used in the policy;
- A statement about how policy violations are to be handled;
- The effective date and dates of any revision.

Policy and procedures documents also should cover:

- The designation of privacy personnel;
- Employee training;
- The distribution of privacy notices to plan participants;
- The rights of plan participants, including
  - No intimidating or retaliatory acts against those asserting their rights,
  - The bar against privacy rights waivers,
  - The ability to amend one's PHI,
  - The ability to get an accounting of PHI disclosures;
- The adoption and implementation of PHI use and disclosure controls, including
  - The "minimum necessary" standard for sharing information,
  - The use of authorizations,
  - Administrative, physical and technical safeguards to secure access to PHI,
  - Verification of the identity of individuals or entities requesting PHI,
  - Recognition of personal representatives,
  - Plan participant access to PHI;
- Other policies and procedures, including
  - Documentation of privacy decisions,
  - PHI disclosures for public health, law enforcement, or legal process,
  - De-identification,
  - Retention of compliance-related records,
  - Handling complaints,
  - Sanctions for employee violations,
  - Violation mitigation.

A. Designating Privacy Personnel and Conducting Personnel Training

Covered dealership health plans must designate a privacy officer to manage compliance implementation, and a contact person to answer questions regarding the privacy notice and to handle any complaints from plan participants. Dealership employees responsible for human resources issues are natural candidates for designation as privacy officers and contact persons.

Plan employees who handle or may handle PHI should be knowledgeable about the Privacy Rule and trained on relevant policies and procedures. Employees who handle more PHI need more training. New employees should be trained within a reasonable time. Employees who handle PHI should be retrained when there are material changes to the health plan's Privacy Rule policies and procedures. Job descriptions should be amended to refer to employees' Privacy Rule obligations. The training requirement may be satisfied by providing copies of the policy and procedures document to the appropriate employees. All Privacy Rule training should be documented.

B. Providing Privacy Notices

Covered plans must provide privacy notices to plan participants informing them of their rights and of the health plan's privacy practices. Privacy notices must describe the ways in which the plan may use and disclose PHI and must list a contact for further information. For fully-insured plans, plan insurers (not their sponsoring dealerships) must provide participants with privacy notices. Self-insured dealership plans, and dealership sponsors of fully-insured plans that receive more than SHI also must provide privacy notices. Notices must be distributed to all current plan participants (notices to employees suffice for their dependents) and to new participants upon or before enrollment. Notices must be revised prior to any material

changes to privacy practices or procedures. Plan participants should be provided with a new copy of the Notice every three years. Privacy notices should be in hard copy, with electronic versions posted on any health plan Website. Written acknowledgments of receipt are recommended but not mandated.

C. Knowing and Respecting the Insured's Rights

All sponsoring dealerships and dealership health plans must allow individuals to exercise their rights under HIPAA. Never intimidate, threaten, coerce, discriminate against, or retaliate against individuals exercising their HIPAA privacy rights or require individuals to waive them. As a general rule, plan participants have the right to access their PHI, request amendments, and receive responses to their requests within 30 days. If an amendment is made, notify the requester and others known to have unamended PHI.

Individuals also may request an accounting of the past six years' PHI disclosures, other than those made for treatment, payment, health care operations, or authorized or requested by the individual. Such requests must generally be responded to within 60 days. *(Payment* includes health plan activities to obtain premiums, provide coverage or benefits, or obtain or provide health care reimbursement, e.g., billing, claims management, health benefits adjudications, risk assessments, eligibility, coverage and medical necessity determinations, utilizations reviews, disclosures to consumer reporting agencies, etc. *Operations* are activities compatible with or directly related to treatment or payment, e.g., internal quality oversight, credentialing, legal services, auditing, general administration, underwriting, etc.)

Individuals have the right to request restrictions on the use or disclosure of their PHI and its confidential communication, but most such requests need not be granted. You must establish how and to whom complaints may be made regarding the dealership's policies and procedures and its Privacy Rule compliance. The procedure must provide for complaint documentation and disposition.

Individuals have the right to have personal representatives act for them with respect to their rights under the law. Take reasonable steps to verify that personal representatives are indeed acting on behalf of the individuals in question and the basis for their authority.

D. Adhering to and Using Disclosure Restrictions

PHI may always be disclosed to the individual involved and when required by law (e.g., workers' compensation). PHI may also always be used or disclosed pursuant to authorization or for enrollment, disenrollment, treatment, payment, and health care operations. ***If a disclosure or use is not otherwise permitted (or if you are unsure), obtain an authorization from the individual***.

Authorizations should describe a particular purpose and may not be used beyond that purpose. Obtain authorizations before using PHI for purposes such as selling mailing lists, making employment decisions, determining life insurance eligibility, or disclosing results of pre-employment physicals or lab tests. Authorizations generally must also be obtained before using or disclosing psychotherapy notes. Authorizations must be informed and voluntary, in writing, clear and unambiguous, and they must have a specific expiration date or event. A copy must go to the authorizing individual, who can revoke authorization at any time. Dealership plan employees designated to discuss health plan benefit or claim information with employees should obtain authorizations before disclosing PHI to others. Absent authorization, plans should never disclose PHI to plan sponsors for the purpose of employment-related actions or in connection with any other plan sponsor benefit or benefit plan.

Although the rule allows for exceptions, ***use, release or request only the least amount of PHI reasonably necessary*** for any particular use, disclosure, or request. You must identify who needs access, which categories of PHI, and appropriate access conditions. For routine and recurring PHI, the policy document should spell out how the use, disclosure, or request will be limited. For all other uses, disclosures and requests, review criteria must be spelled out and used by the dealership plan's privacy officer.

E. Instituting Administrative, Technical and Physical Safeguards

Limit PHI access to as few dealership plan employees as possible, preferably only to designated plan privacy personnel. Employees should be directed to discuss health plan claim or benefit information only with designated personnel. Establish administrative, technical, and physical safeguards to minimize access to and protect PHI (e.g., policies, computer

firewalls, locking doors, securing file cabinets, document shredding, etc.). Employee training is critical. Appropriate sanctions must be set for employees who fail to comply with the plan's Privacy Rule policies and procedures. Document any sanctions applied and, to the extent practicable, mitigate any harmful impacts of failures to comply.

F. Amending Health Plan Documents

Amendments to covered plans must state:

- The permitted and required uses and disclosures of PHI to the plan sponsor;
- That the plan will disclose PHI to the sponsor only upon receipt of a certification that the plan documents have been amended to incorporate the sponsor's policies and procedures document;
- That there is an adequate degree of separation between the plan and the sponsor.

These amendments can be fairly complex and are just one more reason why dealerships should limit the use and disclosure of PHI. Moreover, plan sponsors must provide a certification to their plans to enable the amendment.

G. Executing Business Associate Contracts

Health plans often share PHI with contractors and other business associates, i.e., persons or organizations that perform functions or provide services on behalf of health plans. Examples include Third Party Administrators and accounting, actuarial, consulting, data aggregation, legal, management, and accreditation services. Insurers typically are covered entities but not business associates, except when simply providing administrative services to self-funded plans. Moreover, plan sponsors are not business associates of the plans they sponsor. Health plans must use business associate contracts to obtain assurances regarding the safeguarding of PHI used or disclosed by business associates on behalf of the plan. Health plans are not responsible for monitoring their business associates' compliance, but if a material breach or violation is discovered, action must be taken (including ceasing to share additional PHI).

V. Summary and Conclusion

Privacy Rule compliance obligations vary, primarily according to the types of plans dealerships sponsor or fund, and the degree to which they handle PHI. The Privacy Rule provides a federal compliance floor and generally preempts state laws that are contrary to it. State laws may require stronger privacy protections. Consult competent legal counsel for specific compliance assistance pertaining to your dealership, and for information about applicable state laws. Questions of a general nature may be directed to regulatory@nada.org or 703-821-7040.

Endnotes

1. *Receipts* mean total income (or in the case of a sole proprietorship, gross income) plus cost of goods sold as these terms are defined or reported on IRS Form 1120 for corporations; Form 1120S for Subchapter S corporations; Form 1065 for partnerships; or Schedule C for sole proprietorships. Receipts do not include net capital gains or losses, taxes collected for and remitted to a taxing authority if included in gross or total income, or proceeds from the transactions between a concern and its domestic or foreign affiliates (if also excluded from gross or total income on a consolidated return filed with the IRS).

Self-insured plans should not count the cost of stop-loss coverage when calculating total receipts. ERISA group health plans that do not file federal income tax returns reporting receipts should determine annual receipts using proxy measures. Fully-insured health plans should total the premiums paid for health insurance benefits during the last full fiscal year. Self-insured plans (both funded and unfunded) should total the health care claims paid by the employer, plan sponsor, or benefit fund on the plan's behalf during the last full fiscal year. Plans providing health benefits through a mix of purchased insurance and self-insurance should combine the two measures to determine annual receipts.

2. Dealerships sponsoring fully-insured plans that handle PHI need not provide privacy notices to plan participants, but must develop a Privacy Rule policies and procedures document and must amend their plan documents to reflect that they will:

- Disclose PHI only as permitted by the plan documents or as required by law;
- Not use or disclose PHI for employment-related actions or decisions, or in connection with any other sponsor benefit or benefit plan;
- Ensure that adequate separation of records and employees is established and maintained between the plan and plan sponsor;
- Ensure that business associates agree to abide by the same restrictions/conditions as the plan sponsor;
- Report to the plan any improper use or disclosure of PHI;
- Allow individuals to request and obtain copies of their PHI, and to request to amend their PHI;
- Provide requesting individuals with an accounting of the past six years' PHI disclosures;
- Make internal PHI disclosure practices and records available to HHS.

ACKNOWLEDGMENT

This Bulletin was written by

Douglas I. Greenhaus
Director, Environment, Health and Safety
NADA Legal Department

Some dealerships may require the assistance of legal counsel or a health insurance professional to comply with the rules discussed. The Privacy Rule provides a federal compliance floor and generally preempts state laws that are contrary to it. At the same time, state laws may require stronger privacy protections. Consult competent legal counsel and/or your state or local dealership association for more information regarding applicable state laws.

National Automobile Dealers Association
8400 Westpark Drive
McLean, Virginia 22102-3591
e-mail:me@nada.org
http://www.nada.org
©NADA 2004. All rights reserved.

ATD® American Truck Dealers

To order additional copies of this bulletin,
visit our online catalog at www.nada.org/mecatalog
or call NADA Management Education
(800) 252-NADA, ext. 2, or (703) 821-7227