FDA RELEASES UNIQUE DEVICE IDENTIFICATION FINAL RULE, DRAFT GUIDANCE

On September 24, 2013, the Food and Drug Administration (FDA) published a Final Rule, which will, over the next several years, require many medical devices distributed in the U.S. to carry a unique device identifier (UDI). According to the accompanying FDA Press Release, the UDI system is intended to provide a consistent method of identifying medical devices and improve the quality of information received by the FDA in its medical device adverse event reports, thereby improving patient safety. The FDA also released Draft Guidance for Industry intended to outline the process for submitting information to the UDI system.

The Final Rule comes more than a year after the FDA's July 2012 Proposed Rule requested input from industry, the clinical community and patient and consumer groups regarding device identification and postmarket surveillance. The UDI system also is a key component of the FDA's September 2012 and April 2013 National Medical Device Postmarket Surveillance Plan.

Under the Final Rule, a UDI will be assigned to most medical devices. The UDI will be a unique numeric or alphanumerical code consisting of two components. The first component is the mandatory device identifier (DI) portion, which identifies the manufacturer and specific version or model of a device. The second component is the variable production identifier (PI) portion, which identifies a device's lot or batch number, serial number, expiration date, manufacture date or other similar information.

The Final Rule also creates the Global Unique Device Identification Database (GUDID), a publicly searchable database administered by the FDA to serve as a reference catalogue and include a standard set of basic identifying elements for every device labeled with a UDI. According to the FDA, the UDI does not indicate, and the GUDID will not contain, "protected health information" under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The FDA plans to implement the UDI system in phases, focusing first on high-risk medical devices. Many low-risk medical devices will be exempt from some or all of the requirements of the Final Rule. By September 24, 2014, high-risk medical devices (including most Class III medical devices) generally will be required to carry the UDI on their label and packaging, and manufacturers of these devices will be required to submit data to the GUDID. Devices intended for reuse that require reprocessing before each use also must be permanently marked with a UDI directly on the device. Devices that are implantable, life-supporting or life-sustaining generally will be subject to similar UDI and GUDID requirements. Manufacturers of moderate-risk devices (including most Class II medical devices) will have three years to comply with the provisions of the Final Rule. Manufacturers of low-risk medical devices (Class I medical devices) that are not exempted from UDI requirements will have five years to comply with the Final Rule. However, a Class I device exempted from the FDA’s good manufacturing practices requirements also will be exempted from UDI requirements. In addition, devices manufactured and labeled prior to the FDA's compliance date for that class of devices also are exempt from the UDI.
requirements, but this exemption expires three years after the applicable compliance date.

The FDA's GUDID Draft Guidance for Industry is intended to help manufacturers prepare to submit information to the database. In order to further clarify any issues that may arise during implementation of the GUDID, the FDA has requested comments and suggestions regarding the Draft Guidance. The Draft Guidance also raises important issues regarding provider tracking of UDI information and adverse event reporting. Providers should consider this information in developing recordkeeping and reporting policies and procedures.

If you are interested in submitting comments or suggestions to the FDA, or if you need assistance with medical device tracking and adverse event reporting policies and procedures, please contact Lance L. Shea at lshea@bakerlaw.com or 202.861.1648; or Cory J. Fox at cjfox@bakerlaw.com or 713.646.1358.

**COMPUTER CRIME INSURANCE COVERAGE: CAN IT COVER FRAUDULENT ENTRIES SUBMITTED BY AN AUTHORIZED USER?**


Universal claimed that it suffered approximately $18.3 million in losses from fraudulent claims made against some of its Medicare Part D plans. Most of these claims were submitted by providers directly into Universal's computer system and processed through the system. In some cases, "the perpetrators enrolled new members in the Medicare Advantage plan with the person's cooperation, in return for which the member received a kickback from the provider. In other cases, the provider used the member's personal information without that person's knowledge." The National Provider Identifiers (NPIs) used in some cases were for fictitious providers; in other cases, NPIs were taken fraudulently from legitimate providers. Many of the false claims were automatically adjudicated by Universal American's computer system with no manual review.

The Policy provided coverage for losses resulting directly from a fraudulent entry of electronic data or computer program into, or change of electronic data or computer program within, the insured's proprietary computer system, provided that the entry or change causes (1) property to be transferred, paid or delivered; (2) an account of the insured, or of its customer, to be added, deleted, debited or credited; or (3) an unauthorized account or a fictitious account to be debited or credited.

Universal American argued that the provision covers any fraudulent entry of data, even by an authorized user. National Union, the insurer, contended the Policy only covered acts by unauthorized persons, such as hackers. The appellate court found that the "unambiguous plain meaning" of the Policy, covered losses from a fraudulent "entry of electronic data" or "change of electronic data" within Universal American's proprietary computer system. The court interpreted this language to apply only to wrongful acts in manipulation of the computer system (i.e., by hackers), and that the Policy did not provide coverage for fraudulent data submitted by authorized users. Universal American had argued that the Policy was vague and therefore covered fraudulent entries by authorized users. While the New York case was decided against Universal American, that may not be the case in all states, as insurance contracts typically are construed in favor of the insured.

This case highlights why it is important to closely examine insurance policies, including the insuring agreements, definitions and exclusions. Computer crime insurance policies often may be vague and complicated and slight wording changes can make a significant difference to your right of recovery. Furthermore, the language
used in computer crime policies, in many cases, has failed to keep pace with technological advances and often does not recognize the unique issues faced by healthcare providers. This leaves providers in the difficult position of having to determine the scope of necessary insurance protection and the protection policies provide.

Finally, this type of coverage, in addition to other insurance policies, should not be overlooked by providers when a data breach occurs, as coverage may be present for some or all of the losses incurred, depending upon the wording of the policy and facts surrounding the data breach.

For more information, please contact Robert M. Wolin, rwolin@bakerlaw.com or 713.646.1327; or Lynn Sessions, lsessions@bakerlaw.com or 713.646.1352.

---

**DOL CONTINUES EFFORT TO SUBJECT TRICARE PROVIDERS TO FEDERAL EQUAL EMPLOYMENT OPPORTUNITY AUDITS**

Previously, we reported how the U.S. District Court for the District of Columbia found in *UPMC Braddock v. Harris* that providers of healthcare services are subject to federal equal employment opportunity mandates applicable to government contractors and subcontractors. Today, more than six months later, that decision continues to have legs.

Indeed, a recent decision by the U.S. Department of Labor’s (DOL) Administrative Review Board (ARB) shows how aggressively the Office of Federal Contract Compliance Programs (OFCCP) is pursuing investigations against healthcare providers. The ARB's decision, issued in *OFCCP v. Florida Hospital of Orlando*, also shows how heated the debate has become, with numerous industry groups and civil rights groups lining up on either side of the issue.

TRICARE is a federal government program designed to provide medical and dental care for members of the U.S. armed services, certain former members of the armed services and their dependents. Florida Hospital of Orlando (Hospital) subcontracts with Humana Military Healthcare Services (HMHS) to provide healthcare services for TRICARE beneficiaries. The ARB concluded that the Hospital, HMHS and TRICARE form an "integrated healthcare delivery system."

After the Hospital rebuffed the OFCCP's attempt to conduct an audit of the Hospital's compliance with various equal employment opportunity laws, an Administrative Law Judge (ALJ) ordered the Hospital to comply with the OFCCP's request for information. An appeal to the ARB followed.

The primary issue on appeal was whether the Hospital was a subcontractor under 41 C.F.R. § 60-1.3(1), which defines a "subcontract" as any arrangement between a contractor and any person "[f]or the purchase, sale or use of personal property or nonpersonal services which, in whole or in part, is necessary to the performance of any one or more contracts." In concluding that the Hospital was a subcontractor, the ARB relied upon and embraced several elements of the district court's decision in *UPMC Braddock*.

Addressing the question whether the subcontract between the Hospital and HMHS was for "nonpersonal services," the ARB relied upon and embraced the district court's assessment that determining whether a contract for healthcare services is for "nonpersonal services" requires an examination of the extent to which the prime contractor controls the delivery of services by the subcontractor. The ARB found that even though TRICARE and HMHS impose standards of care and require reporting (including reporting of information regarding medical staff qualifications and privileges), the Hospital operated independently and, therefore, the contract was for nonpersonal services.
In addition, the ARB relied upon *UPMC Braddock* to determine that the work performed by the Hospital was necessary to the performance of HMHS’s contract with TRICARE because, without the Hospital, HMHS could not deliver the services. Finally, looking at *UPMC Braddock*, the ARB rejected the argument that the Hospital had not agreed to be a subcontractor (i.e., thereby agreeing to subject itself to OFCCP jurisdiction).

For all of these reasons, the ARB concluded that the Hospital was a subcontractor.

This decision is not the final word for the Hospital; the ARB remanded the matter to the ALJ for further consideration of the question whether the Hospital is exempt from OFCCP jurisdiction because the payments from the TRICARE program constitute federal financial assistance. Nonetheless, it is becoming clear that the *UPMC Braddock* decision will make it easier for the OFCCP to pursue investigations against healthcare providers who have contracts with entities responsible for providing health services to federal government employees.

Healthcare providers with questions about the impact of this decision are well advised to consult with legal counsel. For more information, please contact Ellen Shadur Gross, egross@bakerlaw.com or 310.442.8816, or any member of the BakerHostetler Healthcare Industry Team.

---

**TELEMARKETING: HIPAA CAN REVERSE THE CHARGES UNDER THE TCPA**

The Telephone Consumer Protection Act (TCPA) generally limits automatically dialed and prerecorded telemarketing calls to wireless and residential phones. In the past, healthcare providers and other "advertisers" could rely on an established business relationship (such as a previous purchase) to circumvent the need to obtain a consumer's written consent to receive certain telemarketing or advertising calls. Beginning October 16, the "established business relationship" exemption for prerecorded telemarketing calls will be eliminated from the TCPA. However, the good news for healthcare providers is that the Federal Communications Commission (FCC) retained the exempt organization exception and also adopted an exemption in this rule for certain automatically dialed and prerecorded healthcare-related calls by or on behalf of a covered entity or its business associates regulated under HIPAA.

The FCC's rules, published on June 11, 2012, for auto-dialed and prerecorded calls made to wireless numbers or to a landline in certain limited circumstances (e.g., call to a patient room of a hospital or other healthcare facility) (Restricted Lines) will now allow such calls if (1) the caller has the express prior consent of the recipient of the call (including prior verbal consent); and (2) the call does not introduce an advertisement and/or constitute telemarketing.

If the call, however, introduces an advertisement and/or constitutes telemarketing, then providers and other advertisers generally will be required to obtain a consumer's prior written express consent for such autodialed or prerecorded calls to a Restricted Line. However, if a telemarketing call to a Restricted Line delivers a "health care" message by or on behalf of a HIPAA-covered entity or its business associate, the new HIPAA exception will apply and the recipient's written consent will not be required. Prior verbal consent, however, will be required. Calls made by or on behalf of a tax-exempt, nonprofit organization likewise generally will require only prior express consent rather than prior written consent. The distinction between telemarketing and nontelemarketing calls can be difficult to discern in some cases. Providers will need to examine their messages carefully and ensure that they know what types of communications they are making in order to obtain the correct consent for calls to a Restricted Line.

The FCC's rules likewise require a recipient's prior written consent for prerecorded calls made to residential phone lines. However, no prior consent is required if the call (1) is made for emergency purposes; (2) is not made for a commercial purpose; (3) is made for a commercial purpose but does not include or introduce an advertisement or constitute telemarketing; (4) is made by or on behalf of a tax-exempt nonprofit organization; or (5) delivers a "health care" message made by, or on behalf of, a "covered entity" or its "business associate."

However, providers should be aware that in instances where a prerecorded healthcare-related call's primary motivation appears to be sending a telephone solicitation or unsolicited advertisement rather than a true healthcare-related message, or in those cases where the call is not covered by HIPAA, as determined by the U.S. Department of Health and Human Services, the restrictions generally applicable under the TCPA will apply "as the facts warrant," according to the FCC's commentary.

The FCC's newly adopted HIPAA exception also exempts prerecorded healthcare-related calls made by, or on behalf of, a "covered entity" or its "business associate," from the FCC's other requirements, such as identification, time-of-day, opt-out and abandoned call requirements. This rule change largely harmonizes the FCC's position with that of the Federal Trade
The FCC also implemented a rule that requires telemarketers to implement an automated, interactive opt-out mechanism for autodailed or prerecorded telemarketing calls to wireless numbers and for prerecorded telemarketing calls to residential lines, which would allow a consumer to opt out of receiving additional calls immediately during a telemarketing robocall. This rule change also largely harmonizes the FCC’s position with that of the FTC’s TSR.

When required, a consumer’s written consent must be signed or electronically signed and be sufficient to show that the consumer (1) received “clear and conspicuous disclosure” of the consequences of consenting (i.e., that the consumer will receive future calls that deliver prerecorded messages by or on behalf of the recipient of the consent); and (2) having received this information, agrees unambiguously to receive such calls at a telephone number the consumer designated. In addition, the written agreement must be obtained “without requiring, directly or indirectly, that the agreement be executed as a condition of purchasing any good or service.” Although prior express consent can be obtained either orally or in writing, the FCC provides little guidance as to how to ensure such consent is documented, leaving it to the caller to determine whether to rely on a verbal consent in complying with its requirements under the rules.

The TCPA has seen an explosive growth in class action litigation over the past few years. This growth has been largely driven by plaintiffs eager to receive the statutory damages of between $500 and $1,500 per violation, without need to prove actual damages. There is no class action cap on the statutory damages under the TCPA. Hence, providers should carefully examine their telemessaging practices.

For more information, please contact Robert M. Wolin, nwolin@bakerlaw.com or 713.646.1327; Lynn Sessions, lsessions@bakerlaw.com or 713.646.1352; or Cory J. Fox, cjfox@bakerlaw.com or 713.646.1358.

COURT OVERTURNS PRE-SUIT PATIENT AUTHORIZATION REQUIREMENT UNDER FLORIDA MEDICAL MALPRACTICE STATUTE

On September 25, 2013, the Northern District Court of Florida, Tallahassee Division, ruled that Florida Statute § 766.1065 violated HIPAA by requiring a plaintiff in a medical malpractice action to deliver a presuit authorization allowing the defending parties to conduct ex parte interviews of plaintiff’s other healthcare providers. Finding that HIPAA does not “otherwise permit or require disclosures in an ex parte interview of the kind at issue,” and that the plaintiff’s “authorization” under applicable Florida law was invalid under federal rules, the court enjoined the defendants from interviewing plaintiff’s other healthcare providers ex parte (1) absent voluntary consent of the plaintiff or (2) in accordance with the provisions of HIPAA.

As background, claimants pursuing medical negligence suits in Florida must meet specific presuit requirements pursuant to Fla. Stat. § 766.106. These presuit requirements are intended to put the defendant on notice of the individual’s intent to sue and thus must be completed before the claimant files his or her complaint for medical negligence. Among other things, the Florida statute requires the claimant to provide to the prospective defendant a list of all known healthcare providers during the two-year period prior to the alleged act of negligence that treated or evaluated the claimant, along with copies of all medical records.

Section 766.1065, which became effective July 1, 2013, also requires the plaintiff to submit a signed authorization allowing the defendant, the defendant’s attorney, insurer and/or adjuster, to interview the plaintiff’s other healthcare providers ex parte. The authorization permits disclosure of protected health information that is potentially relevant to the claim of personal injury or wrongful death and must be in the form specified pursuant to the statute. Please note that the authorization does not give the defendant permission to inquire about all matters of the plaintiff’s health, only those relevant to the plaintiff’s cause of action.

The court based its ruling on two key premises: (1) HIPAA expressly preempts any conflicting state law, except those state laws that are more stringent than HIPAA (i.e., a state law that would prohibit a disclosure otherwise permitted under the federal rules); and (2) while HIPAA addresses disclosures made in connection with judicial or administrative proceedings, it does not supersede the need for a valid authorization provision. Specifically, under HIPAA, valid authorizations must meet specific content requirements. While the court acknowledged that the authorization mandated under the Florida statute met the specified content requirements, the authorization nonetheless failed to show the individual’s consent. Instead, the authorization evidenced only the individual’s mandated compliance with state law.

The court concluded that the defendants were not permitted to conduct interviews or other communications with plaintiff’s other healthcare providers and enjoined the defendants from doing so. This decision, however, is unlikely to be the last word, as the defendants likely will appeal the ruling, and the ultimate resolution of this case remains unclear. Other courts
have reached the opposite conclusion on a similar question of law as demonstrated in In re Collins, M.D., 286 S.W.3d 911 (Tex. 2009). These rulings do show the tension regarding HIPAA preemption.

For more information, please contact Lynn Sessions, lsessions@bakerlaw.com or 713.646.1352; or Anne C. Foster, afoster@bakerlaw.com or 216.861.7258.

EVENTS CALENDAR

October 24

Houston counsel Lynn Sessions will speak on "Mobile Technology: Health Care's Moving HIPAA and HITECH Targets" during a telephone seminar/audio webcast sponsored by The American Law Institute.

Houston partner Donna Clark will speak on "Stark Law Implications of Real Estate Transactions" at the 11th Annual Conference of the Higher Education Real Estate Lawyers in San Diego, California.

November 14

Cleveland counsel Tom Campanella will speak on "Future Opportunities for Innovation in Health Care" at the Global Center for Health Innovation sponsored by the Healthcare Financial Management Association in Cleveland, Ohio.

November 19

Houston counsel Lynn Sessions will speak on "HITECH: The Final Rule" at the Healthcare Educational Workshop sponsored by Beazley in Atlanta, Georgia.

December 5

Cleveland counsel Tom Campanella will speak on "The Affordable Care Act: Where Do We Go From Here?" at the Health Law Lunch Series sponsored by the Cleveland Metropolitan Bar Association in Cleveland, Ohio.