SCHENCK PRICE SMITH & KING, LLP
ATTORNEYS AT LAW
– FOUNDED 1912 –

HEALTH LAW DISPATCH

www.spsk.com

July 2017

Wrongful Disclosure of HIV Status is Subject to Two-Year Statute of Limitations in N.J.

By Meghan V. Hoppe, Esq.

In Smith v. Datla, 2017 N.J. Super. LEXIS 95 (App. Div. July 12, 2017), a three-judge Appellate Division panel ruled that a two-year statute of limitations applies to an HIV-positive patient who claims that his physician improperly disclosed his medical status to a third party without consent.

The case stems from Dr. Arvind Datla's treatment of a patient, given the fictitious name "John Smith," with acute kidney failure. During the treatment, Dr. Datla allegedly disclosed Smith's HIV-positive status in the presence of a third-party. Nearly two years later, Smith filed a suit alleging violations of his common-law right to privacy, medical malpractice and wrongful disclosure of his medical status under New Jersey's AIDS Assistance Act (Act), N.J.S.A. 26:5C-1 to 26:5C-14. These claims are all governed by a two-year statute of limitations set forth in N.J.S.A. 2A:14-2.

In his motion to dismiss, Dr. Datla argued that the claims should be governed by the one-year statute of limitations that applies to claims for defamation. The court disagreed and held that the rules regarding defamation claims would not apply since the information Dr. Datla disclosed to the third person was truthful and did not place Smith in a false light.

The court ultimately held that improper disclosure of a plaintiff's HIV-positive status to a third-party without the plaintiff's prior informed consent constitutes a violation of the Act, an invasion of privacy by public disclosure of private facts, and medical malpractice, thereby warranting the two-year statute of limitations.

For more information, contact Meghan V. Hoppe at mvh@spsk.com, or (973) 540-7351.

OIG Permits Waiver of Cost Sharing For Certain Research Patients

By Daniel O. Carroll, Esq.

In only its second advisory opinion of 2017 (OIG Advisory Opinion No. 17-02), the Office of Inspector General ("OIG") allowed a nonprofit medical center (the "Center"), conducting clinical research for a wound care system ("System") pursuant to Medicare Coverage with Evidence Development protocols, to waive or reduce cost sharing amounts for financially needy Medicare beneficiaries. The Center would not advertise or routinely provide waivers or reductions of cost sharing amounts for the System. Rather, such waivers or reductions would only be available on a case-by-case basis for financially needy research subjects unable to pay such amounts. In order to qualify for such waivers or reductions, the research subject would be required to satisfy the Center's financial need policies.

Based on the facts of the proposed arrangement and the OIG's assessment of the Center's application of its financial need policies, the OIG concluded that the proposed arrangement to waive or reduce cost sharing obligations in this context did not constitute grounds for the imposition of administrative sanctions under the federal anti-kickback statute, nor grounds for the imposition of civil monetary penalties under the prohibition on beneficiary inducements. In fact, the OIG found that this proposed arrangement satisfied the exception to the prohibition on beneficiary inducements and would not constitute "remuneration" under Section 1128A(i)(6)(A) of the Social Security Act. See 42 C.F.R. § 1003.110.

For more information, contact Daniel O. Carroll at doc@spsk.com, or (973) 631-7842.

New Alternative Payment Model Exception to Codey Law

By Divya Srivastav-Seth

On July 13, 2017, and effective as of February 1,2018, Governor Christie signed into law P.L.2017 (c.111), which requires alternative payment models to register with the Department of Health ("DOH") and establishes a new exception for alternative payment models ("APMs") from the New Jersey prohibition against physician self-referrals, N.J.S.A. 45:9-22.5 et. seq., also known as the "Codey Law." Subject to certain exceptions, the Codey Law prohibits referrals of a patient by a practitioner for healthcare services in which the practitioner or the practitioner's family has a significant beneficial interest. The new law adds an exception for APMs which have registered with the Department of Health and allows referrals that a practitioner makes, or directs an employee of the practitioner to make, to a health care service in which the referring practitioner has a significant beneficial interest, when participants in APMs registered with the Department of Health make a bona fide determination that the significant beneficial interest is reasonably related to the alternative payment model standards filed with the Department of Health, provided that the determination is documented and retained for a period of 10 years. See N.J.S.A. 45:9-22.5(c)(5).

The new law defines an APM as a model of payment for health care services operated by Medicare, Medicaid or a health insurance carrier that that:(1) has been filed with the Department of Health ("DOH"), 2) provides for payment for covered professional services earned by participating health care practitioners and health care services based on approved quality measures; (3)(a) requires an alternative payment entity to bear financial risk for monetary losses under the alternative payment model; (b) is a medical home; or (c) is an accountable care organization authorized by the Medicare Shared Savings Program or the Center for Medicare and Medicaid Innovation. An alternative payment entity is defined to mean an entity authorized to receive compensation for the provision of health care on a basis that entails the assumption of financial risk, including but not limited to a licensed organized delivery system. An APM "participant" is an entity identified by a Tax Identification Number through which one or more practitioners may bill a health insurance carrier or other payor that is operating an APM, which alone or together with one or more participants composes an APM. An APM shall be deemed approved by the DOH without further review if authorized and approved by CMS. The DOH would have power to review, and revoke if necessary, each registered alternative payment model at least once every six years to determine whether the participants in the APM have complied with the law and other relevant State and federal laws and regulations, and to ascertain if the APM has resulted in a degradation of quality of the health care provided to patients attributable to the alternative payment model. The DOH has been authorized to adopt any rules and regulations deemed necessary to implement the law.

For more information, contact Divya Srivastav-Seth at dss@spsk.com, or (973) 631-7855.

The Epic 2017 Ransomware Attack: Lessons Learned from WannaCry

By Deborah A. Cmielewski, Esq.

The WannaCry ransomware attack that occurred on May 12, 2017 continues to receive much publicity. This colossal tragedy sent shock waves around the globe, forcing businesses and individuals into a frenzy. The attack was particularly frightening to healthcare entities, whose inability to access data could jeopardize the delivery of patient care. But what caused the attack and what does it all mean for HIPAA covered entities and business associates? Just what is ransomware, anyway?

A ransomware attack occurs when a computer is infected with malicious software that denies users access to their system by encrypting the data. A ransom note appears on the users' screens and the hacker holds the system hostage until a ransom is paid for the decryption key. The hacker requires users to pay the ransom in a cryptocurrency (such as Bitcoin). Notably, experts have advised against paying the ransom and instead directed victims to immediately notify law enforcement.

The WannaCry attack resulted from computer system vulnerabilities. In March of 2017, Microsoft issued a security bulletin and patch for Windows systems under support at that time. Unfortunately, not all system users installed the patch. WannaCry was launched two months later in May, spreading like wildfire and infiltrating exposed systems. For healthcare entities, a ransomware attack raises frightening concerns. In addition to affecting patient care, such an attack can result in a data breach of devastating proportions. A ransomware attack on a system that encrypts electronic protected health information ("ePHI") results in a breach and covered entities and business associates must perform a risk assessment to determine whether there is a low probability that the ePHI has been compromised in accordance with the HIPAA Security Rule. Like all risk assessments, the analysis is fact-sensitive and requires assistance of knowledgeable counsel.

The U.S. Department of Health and Human Services, Office for Civil Rights ("OCR") has continued to issue guidance and awareness documents, including a Quick-Response Checklist for dealing with ransomware attacks or other cyber-related security incidents. Of key importance is immediately reporting the crime to the proper law enforcement authorities and reporting any breaches to OCR in a timely manner. Entities subject to the HIPAA rule should arm themselves by implementing the proper policies and procedures, maintaining current backups and ensuring that they can retrieve their data from backups in the event of a cybersecurity incident. Training on prevention and response to ransomware attacks is crucial and entities must be careful to limit access to ePHI to only those users who require it, in order to comply with HIPAA and avoid dangerous consequences.

For more information, contact Deborah A. Cmielewski at dac@spsk.com, or (973) 540-7327.