SMITH & ASSOCIATES

Offices:

3301 Thomasville Road, Suite 201
Tallahassee, Florida 32308

1499 S. Harbor City Blvd., Suite 202
Melbourne, Florida 32901

Phone:

(321) 676-5555

(850) 297-2006

Website:

www.smithlawtlh.com

Geoffrey D. Smith **March 2, 2015**

HIPAA ENFORCEMENT AND COMPLIANCE: WHAT YOU NEED TO KNOW

HIPAA 101

The Health Insurance and Accountability Act of 1996 (HIPAA) is a federal law that sets forth certain requirements to be followed by healthcare providers and related entities with respect to safeguarding a patient's privacy and security.[1] HIPAA helps to ensure that all medical records, medical billing, and patient account information meet certain standards with regard to documentation, handling, and privacy. Most simply, it requires "covered entities" to protect the privacy of patient information, secure patient health information (physically and electronically), adhere to the "minimum necessary" standard for use and disclosure of patient health information, and specifies patients' rights for access, use and disclosure of their health information.

Following the passage of HIPAA, the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act and the 2013 HHS HIPAA Final Omnibus Rule strengthened and updated the federal HIPAA privacy and security standards. Major revisions included: breach notification requirements, fine and penalty increases for privacy violations, mandating that business associates are directly liable for HIPAA compliance, patients' right to request electronic copies of their health care records, and patients' right to restrict disclosure to health plans for services self-paid in full ("self-pay restriction").

HIPAA's Privacy and Security Rule, along with the relatively recent revisions resulting from the 2009 HITECH Act and 2013 Final Omnibus Rule, are discussed briefly below. [2]

HIPAA Privacy Rule

The HIPAA Privacy Rule, 45 CFR Parts 160-164, regulates the use and disclosure of Protected Health Information ("PHI"). Under HIPAA, a covered entity is not required to obtain consent or authorization to use or disclose PHI for *treatment, payment,* or *health care operations*.[3] While the HIPAA Privacy Rule does not require an individual's consent or authorization for the use or disclosure of PHI for treatment, payment, or health care operations, Florida Statutes imposes a more stringent standard for the use or disclosure of patient information, and requires a written authorization for disclosures other than for treatment purposes, except under certain enumerated circumstances.[4]

When the use or disclosure of PHI is not related to treatment, payment, or health care operations, HIPAA requires a written valid authorization, except under certain enumerated exceptions.[5] In order for the authorization to be valid, certain requirements outlined in HIPAA must be met.[6] The HIPAA Privacy Rule contains several key definitions, listed below:

Business Associate: A person, other than a member of the covered entity's workforce, that, with respect to a covered entity, performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information.[7]

Covered Entity: A health plan, health care clearinghouse, or health care provider who transmits any health information in electronic form in connection with a transaction subject to the privacy rule.[8]

Protected Health Information (PHI): Individually identifiable health information that is transmit-

SMITH & ASSOCIATES

Offices:

3301 Thomasville Road,
Suite 201
Tallahassee, Florida 32308

1499 S. Harbor City Blvd.,
Suite 202
Melbourne, Florida 32901

Phone:

(321) 676-5555

(850) 297-2006

Website:

www.smithlawtlh.com

"Once a covered entity discovers a breach of unsecured PHI, both Florida law and HIPAA require notification to the individual 'without unreasonable delay.'"

HIPAA ENFORCEMENT AND COMPLIANCE: WHAT YOU NEED TO KNOW

ted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.[9] PHI is information related to a patient's past, present, or future physical and/or mental health condition. It includes, but is not limited to, the following information when it is maintained by a healthcare covered entity in order to conduct healthcare treatment, payment, or operations: name, address, birthdate, telephone number, email address, social security number, medical record number, account number, certificate/license number, and several other types of information collected and used by healthcare providers. PHI includes health information about individuals who have been deceased less than 50 years.

Minimum Necessary: When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The minimum necessary requirement does not apply to disclosures to a health care provider for treatment.[10]

HIPAA Security Rule

The HIPAA's Security Rule established a national set of security standards for protecting certain health information that is held or transferred in electronic form.[11] The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of electronic protected health information. While the Privacy Rule concerns those who can have access to PHI, the Security Rule's focus is on ensuring that only those who are entitled to access electronic protected health information (ePHI) gain access to ePHI.

The HIPAA Security Rule applies to covered entities and business associates, as defined above. While the Privacy Rule protects the privacy of PHI, the Security Rule protects PHI that a covered entity creates, receives, maintains or transmits in electronic format. The Security Rule does not apply to PHI transmitted orally or in writing, only electronic PHI.[12]

The Security Rule requires covered entities and business associates to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI. The Rule does not dictate which security measures a covered entity or business associate must use, but requires that they take into account: their size, complexity, and capabilities; their technical, hardware and software infrastructure; the costs of security measures; and the likelihood and possible impact of potential risks to e-PHI.[13] Covered entities must adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule, and must periodically review and update its documentation.

Breach Notification Requirements

The HIPAA Security Rule requires covered entities to notify individuals, the Secretary of HHS under certain circumstances, and in some cases, the media, regarding breaches of unsecured protected health information.[14] Once a covered entity discovers a breach of unsecured PHI, both Florida law and HIPAA require notification to the individual "without unreasonable delay."

Under HIPAA's Security Rule, the outside time limit for individual notification is 60 calendar days, while under the Florida Information Protection Act (FIPA), the outer time limit for notification is 30 days.[15] As Florida's law is more stringent, covered entities should be sure to comply with the shorter timeframe specified in Florida statutes. Additionally, business associates are required to notify covered entities of a breach of unsecured PHI.[16]

Enforcement Overview

The U.S. Department of Health and Human Services Office for Civil Rights (OCR) is responsible for enforcing HIPAA's Privacy and Security Rules. OCR enforces the Privacy and Security Rules by investigating complaints and conducting compliance reviews to determine if covered entities are in compliance.

SMITH & ASSOCIATES

Offices:

3301 Thomasville Road,
Suite 201
Tallahassee, Florida 32308

1499 S. Harbor City Blvd.,
Suite 202
Melbourne, Florida 32901

Phone:

(321) 676-5555

(850) 297-2006

Website:

www.smithlawtlh.com

HIPAA ENFORCEMENT AND COMPLIANCE: WHAT YOU NEED TO KNOW

If OCR accepts a complaint for investigation, OCR will notify the person who filed the complaint and the covered entity named in it. Then the complainant and the covered entity will present information about the incident(s) described in the complaint. Covered entities are required by law to cooperate with complaint investigations.

If a complaint describes an action that could be a violation of the criminal provision of HIPAA (42 U.S.C. 1320d-6), OCR may refer the complaint to the Department of Justice for investigation.

OCR reviews the information, or evidence, that it gathers in each case. In some cases, it may determine that the covered entity did not violate the requirements of the Privacy or Security Rule. If the evidence indicates that the covered entity was not in compliance, OCR will attempt to resolve the case with the covered entity by obtaining: voluntary compliance; corrective action; and/or a resolution agreement.

If the covered entity does not take action to resolve the matter in a way that is satisfactory, OCR may decide to impose civil money penalties (CMPs) on the covered entity. If CMPs are imposed, the covered entity may request a hearing in which an HHS administrative law judge decides if the penalties are supported by the evidence in the case.[17]

Potential Fines

Failure to comply with HIPAA can result in civil *and* criminal penalties.

Civil Penalties[18]

The HITECH Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA) that was signed into law on February 17, 2009, established a tiered civil penalty structure for HIPAA violations (see chart below).[19] The Secretary of the Department of Health and Human Services (HHS) has discretion in determining the amount of the penalty based on the nature and extent of the violation and the nature and extent of the harm resulting from the violation.[20] If the covered entity or business associate does not act with willful neglect and corrects the violation within 30 days, the OCR may not impose any penalty. Timely correction is an affirmative defense.[21]

Criminal Penalties[22]

Covered entities and specified individuals, as explained below, whom "knowingly" obtain or disclose individually identifiable health information in violation of HIPAA may be

HIPAA Violation	Minimum Penalty	Maximum Penalty
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million per identical violation per year
HIPAA violation due to reasonable cause and not due to willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million per identical violation per year
HIPAA violation due to willful neglect but violation is corrected within the 30 day required timeframe	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million per identical violation per year
HIPAA violation is due to willful neglect and is not corrected within the 30 day required timeframe	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million per identical violation per year

SMITH & ASSOCIATES

Offices:

3301 Thomasville Road,
Suite 201
Tallahassee, Florida 32308

1499 S. Harbor City Blvd.,
Suite 202
Melbourne, Florida 32901

Phone:

(321) 676-5555

(850) 297-2006

Website:

www.smithlawtlh.com

"The breach involved an estimated 80 million Anthem customers, and Anthem is potentially liable for up to $1.5 million for the breach under HHS rules."

HIPAA ENFORCEMENT AND COMPLIANCE: WHAT YOU NEED TO KNOW

fined up to $50,000, as well as face imprisonment up to one year. Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to five years in prison. Offenses committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm permit fines of $250,000, and imprisonment for up to ten years.[23]

Covered Entity and Specified Individuals

The DOJ concluded that the criminal penalties for a violation of HIPAA are directly applicable to covered entities—including health plans, health care clearinghouses, health care providers who transmit claims in electronic form, and Medicare prescription drug card sponsors. Individuals such as directors, employees, or officers of the covered entity, where the covered entity is not an individual, may also be directly criminally liable under HIPAA in accordance with principles of "corporate criminal liability." Where an individual of a covered entity is not directly liable under HIPAA, they can still be charged with conspiracy or aiding and abetting.[24]

Recent HIPAA Violations

Anthem Health Insurance Breached Again

In February 2015, Anthem Health Insurance, the nation's second largest health insurance company, reported what is likely the largest health care related breach of HIPAA data to date. The breach involved an estimated 80 million Anthem customers, and Anthem is potentially liable for up to $1.5 million for the breach under HHS rules.[25] The two largest health care breaches to date have been Tricare in 2011, which affected 4.9 million individuals, and Community Hospital Systems in 2014, which involved data from 4.8 million individuals.[26]

According to an Anthem official statement, while there was no evidence that medical information was compromised, the attackers gained access to Anthem's IT system and have obtained information from members such as names, medical IDs/SSN, mailing and email addresses.[27] For this to be considered a HIPAA breach, Protected Health Information (PHI) as defined by HIPAA and HITECH Security Rules would have to be involved. A person's name, address and SSN (identifiers confirmed as part of the Anthem breach) are included within the types of data that comprise PHI, as articulated above.

This is not the first time that Anthem's security was breached resulting in HIPAA violations. Anthem recently agreed to pay HHS $1.7 million to settle an investigation into a separate computer breach that occurred in 2010 and resulted in the disclosure of personal information of approximately 612,000 people.[28] (At the time of the breach, Anthem was known as WellPoint). The HHS found that in 2009 and 2010, WellPoint did not adequately implement policies and procedures to protect unsecured "electronic protected health information" covered by HIPAA, and as a result, names, dates of birth, addresses, Social Security numbers and health information of over 600,000 WellPoint customers was disclosed.[29] According to HHS, the personally identifiable information that HIPAA-covered health plans maintain on enrollees and members, including names and Social Security numbers, is protected under HIPAA, even if no specific diagnostic or treatment information is disclosed.[30]

Other Recent HIPAA Enforcement Actions and Resolutions

The Office for Civil Rights, the HHS division responsible for enforcing HIPAA, has levied more than $25.1 million in fines against healthcare organizations responsible for violating the privacy and security rules.[31] To date, HHS has resolved 21 cases that resulted from breach reports of electronic protected health information. A few of these are highlighted below. For a more comprehensive accounting, please see: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html.

SMITH & ASSOCIATES

Offices:

3301 Thomasville Road,
Suite 201
Tallahassee, Florida 32308

1499 S. Harbor City Blvd.,
Suite 202
Melbourne, Florida 32901

Phone:

(321) 676-5555

(850) 297-2006

Website:

www.smithlawtlh.com

HIPAA ENFORCEMENT AND COMPLIANCE: WHAT YOU NEED TO KNOW

$150,000 HIPAA Settlement Involving Anchorage Community Mental Health Services (ACMHS) (December 2014): Under the settlement agreement, ACMHS will pay $150,000 and adopt a corrective action plan to correct deficiencies in its HIPAA compliance program. OCR opened its investigation after receiving notification from ACMHS regarding a breach of unsecured electronic protected health information (ePHI) affecting 2,743 individuals due to malware compromising the security of its information technology resources. OCR's investigation revealed that ACMHS had adopted sample Security Rule policies and procedures in 2005, but these were not followed. Moreover, the security incident was the direct result of ACMHS failing to identify and address basic risks, such as not regularly updating their IT resources with available patches and running outdated, unsupported software. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/acmhs/acmhsbulletin.pdf.

$800,000 HIPAA Settlement Involving Parkview Health System, Inc. (June 23, 2014): Under the settlement, Parkview agreed to pay $800,000 and adopt a corrective action plan to address deficiencies in its HIPAA compliance program. OCR opened an investigation after receiving a complaint from a retiring physician alleging that Parkview had violated the HIPAA Privacy Rule. Parkview employees left 71 cardboard boxes of medical records unattended and accessible to unauthorized persons on the driveway of the physician's home. In addition to the $800,000 resolution amount, the settlement includes a corrective action plan requiring Parkview to revise their policies and procedures, train staff, and provide an implementation report to OCR. http://www.hhs.gov/news/press/2014pres/06/20140623a.html.

$4.8 million HIPAA Settlement Involving New York Presbyterian Hospital and Columbia University (May 2014): Two health care organizations settled charges that they potentially violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules by failing to secure thousands of patients' electronic protected health information (ePHI) held on their network. The monetary payments of $4,800,000 include the largest HIPAA settlement to date. OCR initiated its investigation of New York and Presbyterian Hospital (NYP) and Columbia University (CU) following their submission of a joint breach report, dated September 27, 2010, regarding the disclosure of the ePHI of 6,800 individuals, including patient status, vital signs, medications, and laboratory results. In addition to the impermissible disclosure of ePHI on the internet, OCR's investigation found that neither NYP nor CU made efforts prior to the breach to assure that the server was secure and that it contained appropriate software protections. http://www.hhs.gov/news/press/2014pres/05/20140507b.html.

$1.7 Million HIPAA Settlement Involving Concentra Health Services (April 2014): OCR opened a compliance review of Concentra Health Services (Concentra) upon receiving a breach report that an unencrypted laptop was stolen from one of its facilities, the Springfield Missouri Physical Therapy Center. OCR's investigation revealed that Concentra had previously recognized in multiple risk analyses that a lack of encryption on its laptops, desktop computers, medical equipment, tablets and other devices containing ePHI was a critical risk. While steps were taken to begin encryption, Concentra's efforts were incomplete and inconsistent over time leaving patient PHI vulnerable throughout the organization. OCR's investigation further found Concentra had insufficient security management processes in place to safeguard patient information. Concentra has agreed to pay OCR $1,725,220 to settle potential violations and to adopt a corrective action plan.
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/stolenlaptops-agreements.html.

What To Do If You Become Aware of a HIPAA Breach?

Covered entities must provide a process for individuals to make complaints and document all such complaints.[32] Additionally, covered entities may not take any retaliatory

SMITH & ASSOCIATES

Offices:

3301 Thomasville Road,
Suite 201
Tallahassee, Florida 32308

1499 S. Harbor City Blvd.,
Suite 202
Melbourne, Florida 32901

Phone:

(321) 676-5555

(850) 297-2006

Website:

www.smithlawtlh.com

"Any person who believes that a covered entity or business associate is not complying with HIPAA has the right to file a complaint with HHS."

HIPAA ENFORCEMENT AND COMPLIANCE: WHAT YOU NEED TO KNOW

actions against anyone making a complaint.

If a breach of unsecured protected health information poses a risk of significant financial, reputational or other harm to the patient, business associates must promptly report the breach to covered entities, and covered entities must notify the patient without unreasonable delay, and no later than within 60 days under HIPAA[33], or 30 days under FIPA. If the breach involves fewer than 500 persons, the covered entity must notify HHS by filing an electronic report no later than 60 days after the end of the calendar year.[34] If the breach involves 500 or more persons, the covered entity must file the electronic report when it notifies the patient.[35] The written notice to the patient must satisfy regulatory requirements.[36]

Documenting proper actions will help you defend against HIPAA claims. Covered entities and business associates are required to maintain documentation required by HIPAA for six years.[37]

Understanding the HIPAA Complaint Process and Compliance Reviews

It is important that covered entities have a working knowledge of the complaint, investigation, and enforcement process in order to ensure HIPAA compliance.[38]

The Complaint

Any person who believes that a covered entity or business associate is not complying with HIPAA has the right to file a complaint with HHS.[39] The complaint must name the provider who allegedly violated HIPAA and describe the acts or omissions that are believed to have violated HIPAA. The statute of limitations time period for filing complaints is 180 days after the date when the complainant knew or should have known that the act or omission occurred, but this time limit can be waived for good cause.[40]

Investigating Complaints

If HHS accepts a complaint for investigation, it will notify the person who filed the complaint and the covered entity named in it. Then the complainant and the covered entity will have the opportunity to present information about the incident described in the complaint. HHS has the authority to subpoena witnesses and documents as part of its investigation. The investigation may include a review of the covered entity's policies, procedures, or practices.[41]

Once HHS has completed its investigation, one of three things may occur. The first thing that may occur is that HHS may close the case in favor of the covered entity because it determines that the covered entity did not violate HIPAA. HHS will inform the covered entity and the complainant of its determination.[42]

Assuming HHS finds that a covered entity has violated HIPAA, HHS will attempt to resolve the matter informally, which could include such things as demonstrated compliance, a completed corrective action plan, or other resolution agreement.[43]

If the complaint is not resolved by informal means, the HHS will inform the covered entity and will allow the covered entity to submit written evidence of any mitigating factors or affirmative defenses.[44] Mitigating factors are things such as the nature of the violation; the circumstances surrounding the violation; the degree of culpability of the covered entity; a history of compliance; and, the financial condition of the covered entity. Affirmative defenses would include circumstances that made it unreasonable for the covered entity, despite exercising ordinary care and prudence, to comply with HIPPA.[45] After considering any mitigating factors and/or affirmative defenses, if HHS finds that a civil money penalty should be imposed, it will inform the covered entity or business associate of such finding in a notice of proposed determination.[46]

Compliance Reviews

In addition, HHS may conduct compliance reviews to determine whether a covered entity or business associate is complying with HIPAA.[47] HHS may initiate these reviews when it becomes aware of possible violations of HIPAA by a covered entity.

SMITH & ASSOCIATES

Offices:

3301 Thomasville Road,
Suite 201
Tallahassee, Florida 32308

1499 S. Harbor City Blvd.,
Suite 202
Melbourne, Florida 32901

Phone:

(321) 676-5555

(850) 297-2006

Website:

www.smithlawtlh.com

HIPAA ENFORCEMENT AND COMPLIANCE: WHAT YOU NEED TO KNOW

How to Protect Yourself and Avoid Penalties

Cyber attacks on health care organizations increased 100 percent between 2009 and 2013, and about 40 percent of health care organizations reported facing criminal cyberattacks in 2013.[48] The FBI released a warning to the health care sector in April 2014, advising health care providers that their cybersecurity systems lagged behind protections in the retail and financial sectors, leaving them vulnerable to attacks by hackers.[49]

Healthcare organizations should perform a HIPAA risk assessment to look at where patient information is stored and accessed, and how the organization protects that information. Such an assessment will examine the risks of a breach and provide recommendations on how to minimize risks. Every health care organization should protect its sensitive data by doing the following:

- Perform a security risk analysis yearly to discover security vulnerabilities
- Keep hardware and software updated with current security patches
- Determine whether the use of encryption technology is reasonable and appropriate, and if so, deploy encryption technology
- Perform routine audits of access to information

Additionally, it is important that every organization engage in a full compliance review of policies, forms, and procedures on an annual basis with health care regulatory counsel to ensure HIPAA compliance. All "covered entities" and "business associates" were required to update their HIPAA policies, procedures, forms, and Notices of Privacy Practices by September 23, 2013. All covered entities must have documented policies and procedures regarding HIPAA compliance. Additionally, HIPAA compliance requires staff privacy and security training on a regular basis.

As discussed above, HIPAA compliance is mandatory and fines for breach are hefty. HIPAA regulatory counsel can help to ensure HIPAA compliance by reviewing, revising, and updating internal HIPAA policies and procedures, and tailoring such policies and procedures to the specific health care entity. At a minimum, to avoid HIPAA penalties, health care providers and business associates should:

- **Designate HIPAA Privacy and Security Officers.** Covered entities must designate privacy and security officers responsible for ensuring HIPAA compliance. These individuals, among other things, will be responsible for the development and implementation of policies and procedures and for receiving HIPAA complaints. The designations must be documented in writing.[50]

- **Provide Appropriate Training to Employees and Agents.** Covered entities and business associates must train their employees to comply with HIPAA policies and procedures, and all trainings should be documented in order to avoid/minimize HIPAA penalties.[51]

- **Ensure Compliance with Authorization, Use, and Disclosure Rules.** As discussed above, covered entities and business associates may not use, access, or disclose protected health information without the patient's valid, HIPAA-compliant authorization unless the use or disclosure fits within an exception.[52] Authorization is not required under HIPAA to carry out treatment, payment, or health care operations, however Florida Statutes requires a more stringent standard in some circumstances, and a covered entity would be required to adhere to both.

- **Know Patients' Rights.** Covered entities and business associates must understand and adhere to HIPAA's patients' rights.[53]

- **Maintain HIPAA Compliant Written Policies and Forms.** Covered entities and business associates must develop and maintain written policies

SMITH & ASSOCIATES

Offices:

3301 Thomasville Road,
Suite 201
Tallahassee, Florida 32308

1499 S. Harbor City Blvd.,
Suite 202
Melbourne, Florida 32901

Phone:

(321) 676-5555

(850) 297-2006

Website:

www.smithlawtlh.com

HIPAA ENFORCEMENT AND COMPLIANCE: WHAT YOU NEED TO KNOW

that implement the privacy and security rule requirements, including those dealing with confidentiality and patients' rights.[54]

- **Execute Compliant Business Associate Agreements**. HIPAA requires covered entities to execute "business associate agreements" with their business associates before disclosing protected health information to the business associate.[26] To avoid liability for the business associate's actions, covered entities must ensure that their agreements specify that the business associate is an independent contractor and not an agent of the covered entity.

- **Implement Appropriate Safeguards for PHI and ePHI.** A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.[55] The security rule contains detailed regulations concerning safeguards that must be implemented to protect electronic health information.[56]

- **Respond Immediately to Any Breach.** HIPAA requires covered entities and business associates to investigate any privacy complaints, mitigate any breach, and impose appropriate sanctions against any agent who violates HIPAA.[57] A covered entity or business associate can avoid HIPAA penalties altogether if it does not act with willful neglect and corrects the violation within 30 days.

Geoffrey D. Smith is a shareholder in the law firm of Smith & Associates, and has practiced in the area of health care law for over 20 years.

[1] See Pub.L. No. 104-191, 110 Stat.1936 (1996) (codified at 42 U.S.C. § 1320d-d8), commonly referred to as the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
[2] For additional information on HIPAA Privacy and Security Rules, see http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html and http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html
[3] 45 C.F.R. §164.502.
[4] § 456.057(7)(a), Florida Statutes. While beyond the scope of this article, it is imperative that covered entities familiarize themselves and comply with the more stringent Florida statutes governing patient privacy and security, and the recently enacted Florida Information Protection Act of 2014 (FIPA), which took effect July 1, 2014.
[5] 45 C.F.R. §164.508.
[6] 45 C.F.R. §§164.508, .512.
[7] 45 C.F.R. §160.103.
[8] 45 C.F.R. §160.103.
[9] 45 C.F.R. §160.103.
[10] 45 C.F.R. §164.502(b).
[11] http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html.
[12] http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html.
[13] 45 C.F.R. §164.306(b)(2).
[14] 45 C.F.R. §§164.404, 164.406, 164.408.
[15] Florida Information Protection Act (FIPA); Fla. Stat. §501.171.
[16] 45 C.F.R. §§164.410.
[17] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/howocrenforces.html.
[18] 45 C.F.R. §160.404.
[19] See http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page.
[20] Id.
[21] 45 C.F.R. §160.410.
[22] 42. U.S.C. §1320d-6.
[23] Id.
[24] See http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page.
[25] http://www.usatoday.com/story/tech/2015/02/05/anthem-health-care-computer-security-breach-fine-17-million/22931345/.
[26] http://www.usatoday.com/story/tech/2015/02/05/anthem-health-care-computer-security-breach-fine-17-million/22931345/.
[27] Id.

SMITH & ASSOCIATES

Offices:

3301 Thomasville Road,
Suite 201
Tallahassee, Florida 32308

1499 S. Harbor City Blvd.,
Suite 202
Melbourne, Florida 32901

Phone:

(321) 676-5555

(850) 297-2006

Website:

www.smithlawtlh.com

[28] http://www.usatoday.com/story/tech/2015/02/05/anthem-health-care-computer-security-breach-fine-17-million/22931345/
[29] Id.
[30] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/wellpoint-agreement.html
[31] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/wellpoint-agreement.html
[32] 45 C.F.R. §164.530.
[33] 45 C.F.R. §164.404.
[34] 45 C.F.R. §164.408(c).
[35] 45 C.F.R. §164.408(b).
[36] 45 C.F.R. §164.404.
[37] 45 C.F.R. §164.530(j).
[38] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/howocrenforces.html
[39] 45 C.F.R. §160.306(a).
[40] 45 C.F.R. §160.306(b)(3).
[41] 45 C.F.R. §160.306.
[42] 45 C.F.R. §160.312(b)
[43] 45 C.F.R. §160.312(a).
[44] 45 C.F.R. §160.312(a).
[45] 45 C.F.R. §160.410.
[46] 45 C.F.R. §160.312.
[47] 45 C.F.R. §160.308.
[48] http://www.washingtonpost.com/blogs/the-switch/wp/2015/02/05/why-hackers-are-targeting-the-medical-sector/?hpid=z1.
[49] Id.
[50] 45 C.F.R. §164.530(a).
[51] 45 C.F.R. §164.530(b).
[52] 45 C.F.R. §164.502.
[53] 45 C.F.R. §§164.524, .526, .528.
[54] 45 C.F.R. §164.316.
[55] 45 C.F.R. §164.530(c).
[56] 45 C.F.R. §164.308.
[57] 45 C.F.R. §164.530.

SMITH & ASSOCIATES

Offices:

3301 Thomasville Road,
Suite 201
Tallahassee, Florida 32308

1499 S. Harbor City Blvd.,
Suite 202
Melbourne, Florida 32901

Phone:

(321) 676-5555

(850) 297-2006

Website:

www.smithlawtlh.com

Update on Return of Nursing Home CON in Florida

"An existing provider that intervenes within 21 days of the publication of the Notice of Decisions has full party status; however, an intervenor that does not intervene within 21 days is only granted status that is contingent"

SMITH & ASSOCIATES

Offices:

3301 Thomasville Road,
Suite 201
Tallahassee, Florida 32308

1499 S. Harbor City Blvd.,
Suite 202
Melbourne, Florida 32901

Phone:

(321) 676-5555

(850) 297-2006

Website:

www.smithlawtlh.com

Update on Return of Nursing Home CON in Florida

"By statute, a party requesting a hearing has a right to demand that the hearing be commenced within 60 days of assignment to an ALJ. As a practical matter, most hearings are not done on this expedited schedule."