DOJ Announces New Initiative to Use False Claims Act to Enforce Compliance with Data Privacy and Security Laws and Contract Requirements

The Department of Justice recently announced the launch of its new Civil Cyber-Fraud Initiative (the "Initiative") which intends to use the False Claims Act to pursue "cybersecurity-related fraud by government contractors and grant recipients."

Specifically, the Initiative will target those who:

1. knowingly provide deficient cybersecurity products or services,
2. knowingly misrepresenting their cybersecurity practices or protocols, or
3. knowingly violate obligations to monitor and report cybersecurity incidents and breaches.

This new initiative significantly expands the potential liability of federal contractors and healthcare provider that participate in federal healthcare programs related to data privacy and cybersecurity issues.

False Claims Act

The False Claims Act broadly prohibits anyone from, among other things, knowingly presenting, or "causing to be presented" a false claim for payment if the claim will be paid directly or indirectly by the federal government. The False Claims Act is the government's main enforcement tool for fighting healthcare fraud, with over $2.2 billion recovered in 2020. Penalties for False Claims Act violations include three times the actual damages sustained by the government, mandatory civil penalties of between $11,181 and $22,363 for each separate false claim, and attorneys' fees and costs. Further, the False Claims Act allows whistleblowers to bring lawsuits on behalf of the federal government. Also known as a "qui tam" realtor, a whistleblower who brings a successful *qui tam* action can receive 15 to 30 percent of the damages the government recovers from the defendants. The ability for an individual within one's own organization to raise flags with the federal government under the False Claims Act especially heightens risk.

HIPAA

Pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), "covered entities" and their "business associates" are subject to certain obligations and limitation related to their use and disclosure of "protected health information" ("PHI"). Covered entities are health care providers, health plans and health care clearing houses that transmit any information in an electronic form in connection with a transaction for which HHS has adopted standards. A business associate is a person or entity that performs certain services for or functions on behalf of the covered entity that involve the use or disclosure of PHI. Finally, PHI is any individually identifiable

information, including demographic data, that relates to an individual's past, present or future health or payment for the provision of healthcare.

The obligations imposed on covered entities and business associates under HIPAA include maintaining and following specific privacy and security policies and procedures regarding access to, use, processing, transfer, storage, and disclosure of PHI and implementing physical, technical, and administrative safeguards to protect the privacy and security of PHI. In addition, covered entities are required to notify affected individuals, the Department of Health and Human Services, and, for certain larger breaches, the media of data breaches. Similarly, business associates are required to notify covered entities of data breaches.

Implications

The goal of holding accountable those who "knowingly provide deficient cybersecurity products or services, knowingly misrepresent their cybersecurity practices or protocols, or knowingly violate obligations to monitor and report cybersecurity incidents and breaches" presents particular risk for covered entities and their business associates.

For example, consider a revenue cycle management ("RCM") company that submits claims on behalf of a healthcare provider (including claims to government payors) that experiences a security incident, conducts a HIPAA risk assessment, and shares that assessment with the Covered Entity customer who determines the RCM company did not implement the necessary physical, technical and administrative safeguards required under HIPAA. Could the customer, the government, or a whistleblower allege that the RCM company knowingly misrepresented its cybersecurity practices or protocols and thereby caused the submission of false claims?

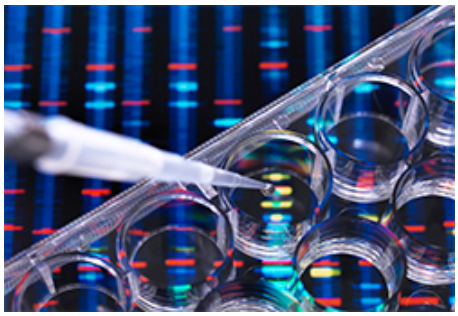
Further, consider an electronic health records company ("EHR") that is certified by the Office of the National Coordinator who experiences a breach of unsecured PHI, conducts a HIPAA risk assessment and determines it is not obligated to report the breach based on a low risk of compromise in accordance with 45 C.F.R. 164.402. Could the government or a whistleblower allege that the EHR company failed to report a breach and thus caused the submission of false claims by healthcare providers that use its EHR and are able to avoid reductions in Medicare reimbursement by using a certified EHR?

False Claims Act cases are commonly pursued under what is known as the "false certification theory". A claim is considered false when a claimant "certifies compliance with a statute or regulation as a condition to governmental payment." The false certification theory considers a claimant's *request* for payment as "implied certification" of compliance with said statutes or regulations. Despite the broad implications of the false certification theory, there is some check on the ability of the government or a whistleblower to bring cases on failure to comply with HIPAA through what is known as the materiality requirement under the False Claims Act. In *Universal Health Services v. United States ex rel. Escobar*, the U.S. Supreme Court held that the government and whistleblowers bear the burden of proving the "rigorous and demanding" materiality requirement under the False Claims Act. The Supreme Court further stated that the False Claims Act is "is not a means of imposing treble damages and other penalties for *insignificant* regulatory or contractual violations." Accordingly, the government and whistleblowers must demonstrate that allegedly insufficient technical safeguards or that an alleged failure to report a breach are actually *material* to the government's payment decision.

The potential use of the False Claims Act to enforce HIPAA compliance may also change how due diligence is conducted on covered entities who bill government payors and their and business associates. While security incidents are common, the potential for liability under the False Claims

Act related to such an incident increases the importance of conducting thorough diligence related to such incidents. The importance of conducting due diligence on a seller's compliance with HIPAA's requirements related to administrative, technical, and physical safeguards is also magnified by the potential for liability under the False Claims Act for failure to comply with those requirements. The risk related to conducting a risk assessment related to a data breach is similarly increased and such assessments should be scrutinized carefully in due diligence.

Florida Joins List of States Requiring Licensure for Genetic Counselors



Many allied health professionals are subject to state-level licensing requirements that can vary from jurisdiction-to-jurisdiction. What may be required in New York to hold a medical professional license may differ dramatically from what is required in Illinois or Texas, for instance. One state's requirements may be onerous and administratively taxing; another state's requirements to serve as the same type of medical professional may be quite simple. Assessing licensing requirements for medical professionals from state to state can also involve rapid change, with state legislatures and state licensing boards revising and changing standards on a regular basis.

Most recently, Florida has joined a number of states that require the licensure of genetic counselors by the Florida Department of Health. Genetic counselors play an increasingly important role in the delivery of care. These professionals hold specialized training in genetics and help patients better understand family history, heredity, and how conditions can arise. Genetic counselors can also aid family members in making better and more knowledgeable choices when it comes to selecting patient care, assisting with questions about the most appropriate testing, educating about genetic disorders, and even helping people cope with troubling diagnoses. The **National Society of Genetic Counselors** ("NSGC") describes genetic counselors as "not doctors" but having advanced training in medical genetics and counseling to guide patients on inherited diseases and conditions. Given this advanced training, and given the critical role that genetic counselors can play with patients, according to NSGC, at least 30 states require licensure for the practice of genetic counseling, Florida being the latest state to join this list.

The New Florida Genetic Counseling Licensing Requirement. Florida's **Genetic Counseling Workforce Act** **(the "Law")**, which became effective on July 1, 2021, requires genetic counselors to meet specific qualifications and examination requirements and to register to hold a genetic counseling license. The Law defines "genetic counseling" to include activities such as: obtaining and evaluating individual, family, and medical histories to determine genetic risk for genetic or medical conditions and diseases in a patient, his or her offspring, and other family members; Integrating genetic laboratory test results and other diagnostic studies with personal and family medical history

to assess and communicate risk factors for genetic or medical conditions and diseases and providing written documentation of medical, genetic, and counseling information for families and health care professionals. The Law prohibits the unlicensed practice of genetic counseling, calling it a second degree misdemeanor to, among other things, "[p]ractice genetic counseling or hold [oneself] out as a genetic counselor or as being able to practice genetic counseling or to render genetic counseling services without a license," unless specifically exempted. § 483.916. This is a broadly worded prohibition and could very conceivably be applied to out-of-state practitioners. The only exemptions are for commissioned medical officers in the U.S. Armed Forces or Public Health Service or health care practitioners (like physicians, nurses, or physicians assistants) operating within the scope of his or her license.

For those who are required to register and hold a Florida genetic counseling license, the Law requires that an individual (1) has a master's degree in genetic counseling or a doctoral degree from a medical genetics training program; and (2) has passed an examination to be certified by such by either the American Board of Genetic Counseling, the American Board of Medical Genetics or Genomics, the Canadian Association of Genetic Counsellors, the American Board of Medical Genetics and Genomics or the Canadian College of Medical Geneticists.

The Telehealth Gap. Genetic counseling is unique in that evaluating a patient's health and family history and genetic test results could be done almost entirely via telehealth technologies. Genetic counselors could conceivably see patients all over the country and deliver equally effective services whether someone is next door or several time zones away. But, the law includes a gap: under the new Florida Law, the legislature did not add genetic counseling to the list of Florida's telehealth providers.

The Law's failure to include genetic counselors on the list of Florida's "**telehealth providers**" (Florida Statute Sec. 56.47(1)(b)) is quite likely a legislative oversight and is not intended to prohibit genetic counselors from leveraging telehealth technologies to deliver their services. As written, however, under the new Law, if genetic counselors do employ telehealth to deliver genetic counseling services to patients in Florida, it could technically be found to fall outside the scope of practice and could conceivably be considered the unlicensed practice of genetic counseling, which is a misdemeanor (FL Stat. §§ 483.916(2)).

This concern is highlighted when it comes to out-of-state genetic counselors. The Law does not distinguish between in-state and out-of-state genetic counselors. This means that out-of-state genetic counselors may also find themselves subject to the Law's background and registration requirements if providing services to Florida residents. In fact, the Law does not require that applicants for licensure be Florida based or pass a Florida specific exam. The examinations required for licensure are national and international board exams. Accordingly, an out-of-state genetic counselor would most likely be required to obtain licensure to provide services to Florida residents. But, taken together with the Law's silence on telehealth usage, this means that a genetic counselor based elsewhere in the country could conceivably register as a genetic counselor in Florida but not be able to use telehealth technologies to deliver that care.

Next Steps. The Florida Department of Health's **genetic counseling licensing page is available here**. We will continue to monitor if Florida legislature updates the Law to add genetic counselors to the definition of telehealth providers, and whether the state issues additional guidance for out-of-state practitioners and the requirements they must meet. We will also continue to assess whether other states will join Florida in requiring licensure for genetic counselors.