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.

EDPB Clarifies Scientific Research GDPR Compliance; Key Questions for US Sponsors Remain

Last month, the European Data Protection Board ("EDPB") issued **additional guidance** on the application of the General Data Protection Regulation ("GDPR") in the area of scientific health research. You can read our summary of the **key takeaways here.** While the EDPB's responses offer some clarifications, many obstacles and complications remain for controllers located in the US in a post-**Schrems-II** world. Fundamental principles that are well settled in the US, including what is and what is not considered human subjects research, and what future uses require consent under US regulations, may be at odds with the approach in the EU under the GDPR. US-based controllers should consider the following when planning trials in the EU or UK:

- **Further processing of previously collected data:** The EDPB confirmed that controllers may obtain individuals' consent for future secondary research without specifically defining the research, so long as the purposes of the research are compatible with the *purposes of the original data processing* and adequate safeguards are implemented. Accordingly, while US-based sponsors might be accustomed to freely using de-identified data for research purposes unrelated to the original purpose for which the data was collected, these broad unrelated uses may be subject to restrictions under GDPR.
- **Broad consent:** In the US, sponsors can rely on broad consent for storage, maintenance, and secondary research use of identifiable private information or identifiable biospecimens. However, the EDPB confirmed that broad consent "cannot be asked and relied on for processing health data for any kind of – unspecified – future research purposes" where the scope of the secondary research is not closely related to the original research purpose for which it was collected.**[1]** These broad consent limitations can cause complications for US sponsors who are accustomed to relying on broad consent for future unspecified research. Broad consent limitations under GDPR may further restrict the downstream use or sale of de-

identified biospecimens and data for future unrelated research.

- **Anonymized versus pseudonymized data:** US sponsors commonly assume that because health research data has been key-coded and de-identified in accordance with HIPAA standards (if applicable), and they do not maintain the key (but a third party does), that the data has been "anonymized" and is not subject to regulation. At that point, the key-coded data can be used for any purpose. However, the GDPR regulates even pseudonymised data, which can be a surprise for US sponsors accustomed to the HIPAA regime. The EDPB has reiterated that where key-codes exist, and are maintained by a site, investigator, or other third party processor, it is reasonably likely that the individual could be re-identified. As a result, the key-coded data is still subject to GDPR protections. The EDPB plans to issue future guidance as to whether further downstream recipients of key coded data, who are not permitted to access the key, can consider that data to be anonymized. This guidance will be crucial for research collaborators or specialized research labs who may receive key-coded data for which they have no intent, need, or ability to re-identify data.
- **Transfer of research data and biospecimens:** The transfer of research data and biospecimens into the US for processing remains an ongoing and unsettled concern. Transfers of personal data are restricted unless a US based controller can demonstrate adequate safeguards have been implemented to ensure the rights of the data subjects have been protected. Most of those specific safeguards are either inapplicable to US controllers, or are unduly burdensome for smaller entities to comply with. EDPB is expected to release future guidance to address the question of whether US or other controllers can rely on the legitimate interest derogation for transfer of special categories of data for research purposes.

Conducting scientific health research in the EU raises specific and difficult considerations for US sponsors, including assessing legal bases for processing sensitive data and transfer mechanisms to ensure data is processed in accordance with GDPR. This is not helped by the lack of clarity in the EU around some key issues discussed in this blog. Until the EDPB issues further clarifications, US controllers and trial sponsors are encouraged to consult with counsel to navigate the complexities of EU scientific health research.

---

[1] EDPB Document on response to the request from the European Commission for clarifications on the consistent appliable of the GDPR, focusing on health research, 2 Feb. 2021, response 31.