The Pulse

Tucker
the Health Law Group of Ellis LLP

Arbitration Agreements in Long-Term Care Facilities: CMS Dismisses Appeal of Injunction and Issues New Proposed Rule

June 2017

On Friday, June 2, the Centers for Medicare & Medicaid Services (CMS) retreated from its appeal of a federal court decision that temporarily blocked CMS's ban on pre-dispute arbitration agreements in the Long-Term Care (LTC) setting.

The ban, announced by CMS in fall 2016, was a major shift in the use of arbitration agreements in LTC facilities. In essence, after November 28, 2016, LTC facilities were prohibited from both entering into pre-dispute agreements for binding arbitration with any resident and requiring that a resident sign an arbitration agreement as a condition of admission to the facility. 45 CFR 483.70(n)(1). For LTC facilities that wished to continue their participation in the Medicare and Medicaid programs, they could enter into a binding arbitration agreement only *after* a dispute arose between the parties. 45 CFR 483.70(n)(2). In the event that such an agreement was used, it was subject to certain criteria set out by CMS. 45 CFR 483.70(n)(i)-(vi).

Shortly after CMS announced its Final Rule, the American Health Care Association (AHCA) sought relief from the ban in a Mississippi federal court. *See American Health Care Association, et al., v. Burwell, et al.*, Case No. 3:16-cv-233 (N.D. Miss.). AHCA advocated that CMS did not have the authority to dictate when parties could enter into an arbitration agreement. The court agreed and granted AHCA's request for a preliminary injunction. In its lengthy opinion, the court scrutinized CMS's cited justification for the ban and the rush to its "immediate" effective date.

In response, CMS issued a memorandum to its surveyors in December 2016 that suspended enforcement of the ban "until and unless the injunction is lifted." *See* Centers for Medicare & Medicaid Services, *Long-Term Care (LTC) Regulation: Enforcement of Rule Prohibiting Use of Pre-Dispute Binding Arbitration Agreements is Suspended so Long as Court Ordered Injunction Remains in Effect* (Dec. 9, 2016) available here.

CMS simultaneously appealed the lower court's decision to the United States Court of Appeals for the Fifth Circuit (USCA Case No. 17-60005). The briefing schedule for the appeal was slightly extended at CMS's request, and instead of filing its petitioner's appeal brief on June 2, CMS filed a voluntary dismissal without any cited reason.

Currently, the future of CMS's ban on pre-dispute arbitration agreements looks unpromising. CMS already published a new proposed rule that intends to revise the requirements for LTC facilities' arbitration agreements. *See* 82 Fed. Reg. 26649, available here. The proposal entirely removes the prohibition on pre-dispute agreements; however, CMS is still attempting to impose additional requirements around the contractual process in an effort to "support the resident's right to make informed choices about important aspects of his or her healthcare." CMS is accepting comments on its revised proposed rule until August 7, 2017.

Victoria Vance
Chair
216.696.3360
victoria.vance@tuckerellis.com

William Berglund
Counsel
216.696.2698
william.berglund@tuckerellis.com

Kelli Novak
Associate
216.696.5796
kelli.novak@tuckerellis.com

HHS Task Force Report Offers More Than 100 Recommended Actions to Address the Unique Cybersecurity Challenges Facing the Health Care Industry

The health care industry faces an "urgent challenge" to secure and protect itself against cybersecurity threats as it continues to become more digitally connected, according to the Health Care Industry Cybersecurity Task Force (the "Task Force") in its final report to Congress released in June 2017. In its "Report on Improving Cybersecurity in the Health Care Industry" (the "Report"), the Task Force addresses the challenges that make the health care industry particularly prone to cyberattacks and other incidents, including the "open, sharing culture" required for effective patient care, the value of health care data to hackers and other criminals, and the potential threats to patient safety caused by ransomware and other attacks like the recent WannaCry outbreak in the United Kingdom in May 2017 that can disrupt and even shut down patient care. These challenges require solutions specifically tailored to the realities of today's health care industry. The Report provides a comprehensive diagnosis of the state of health care cybersecurity, details the specific risks that the industry faces, and outlines six high-level imperatives, with corresponding proposed recommendations and action items, that "must be achieved to increase security within the health care industry."

Background

The Task Force, which was established by Congress as part of the Cybersecurity Act of 2015, reflects a public-private partnership whose membership is composed of leaders from all facets of the health care industry, including the federal government, hospitals, insurers, patient advocates, security companies, pharmaceutical and medical device manufacturers, health IT developers and vendors, and laboratories. *Report*, at 5. Congress directed the Task Force to analyze and address the following six issues as part of its work:

1. How other industries have implemented strategies and safeguards for addressing cybersecurity risks within those industries;
2. The challenges and barriers faced by non-government entities in health care in developing cybersecurity protections;
3. The cybersecurity challenges presented to ensure that medical devices and other software or systems are securely connected to electronic health records and networks;
4. Information that should be disseminated to all industry stakeholders, regardless of size, to improve their preparedness for and response to cybersecurity threats impacting the health care industry;
5. Establishment of a plan to allow public and private information-sharing regarding cyber threats and defensive measures; and
6. Reporting to Congressional committees the Task Force's findings and recommendations.

The Report is the product of public meetings, consultations with experts, public responses to blog posts, and internal Task Force meetings throughout 2016 and early 2017.

Unique Cybersecurity Challenges Faced by the Health Care Industry

In its Report, the Task Force set forth the specific cybersecurity challenge facing the health care industry:

> The health care system cannot deliver effective and safe care without deeper digital connectivity. If the health care system is connected, but insecure, this connectivity could betray patient safety, subjecting them to unnecessary risk and forcing them to pay unaffordable personal costs. Our nation must find a way to prevent our patients from being forced to choose between connectivity and security.

Id., at 1. Patient data collected to improve medical care and develop new treatments is highly desirable to private and nation-state hackers, employees with criminal or other malicious intent, and others who may want to commit identity theft, fraud, or the theft of research and proprietary information. The ever-increasing use of medical devices, smart phones, and other products that connect to the Internet and hospital networks as part of patient care present special cybersecurity challenges to patient safety and care. Further, as the Report notes, the health care industry "is a mosaic" of health care providers of all shapes and sizes with varying financial and personnel resources, infrastructure, expertise, and technical capabilities. *Id*. at 1-2. According to the Task Force, health care cybersecurity is "a key public health concern that needs immediate and aggressive attention" and requires an ongoing "public-private partnership" to address the challenges and implement the solutions required to ensure security and patient safety. *Id*. at 2-4.

Imperatives, Recommendations, and Action Items

In addition to providing a detailed diagnosis of the current state of cybersecurity within the health care industry, the Task Force sets forth six imperatives that organize more than 100 recommended actions addressed to a wide range of industry stakeholders. *Id*. at 21-53. The imperatives and some of the key recommendations can be summarized as follows:

1. **Define and streamline cybersecurity leadership, governance, and expectations (Imperative 1).** This includes the creation of a cybersecurity czar role within the U.S. Department of Health and Human Services to coordinate all health care cyber activities (Recommendation 1.1). The Task Force also calls for the harmonization of existing and future federal and state laws and regulations related to cybersecurity that govern the health care industry (Recommendation 1.3) and urges Congress to change federal anti-kickback laws so that large health care organizations can feel safe in sharing cybersecurity resources and information with their partners (Recommendation 1.5). *Id*. at 22-27.
2. **Increase medical device and health IT security and resilience (Imperative 2).** The Task Force's recommendations include securing legacy medical devices and EHR applications that may not have ongoing hardware and software support from the vendors that provided the products (Recommendation 2.1). It also calls for increasing the adoption and rigor of risk management throughout the lifecycle of medical devices and EHRs (from development through end of life recycling or disposal) and across all supply-chain levels (Recommendation 2.3). *Id*. at 28-34.
3. **Develop a sizable workforce with the required technical capability to meet the cybersecurity challenges unique to the industry (Imperative 3).** The Task Force's recommendations include prioritizing and improving cybersecurity leadership roles within health care organizations (Recommendation 3.1) and the development of industry models and federal government incentive programs to ensure that small and medium-size health care providers have robust, state-of-the-art cybersecurity capabilities similar to larger organizations (Recommendations 3.3 and 3.4). *Id*. at 35-39.
4. **Increase cybersecurity awareness and education within the health care industry (Imperative 4).** The Task Force focused this section on recommendations designed to help organizations create a holistic, collaborative approach to cybersecurity where all members of the organization from top to bottom are educated and treat these issues with the sincerity and importance required. Recommendations include education programs targeting organization executives and boards (Recommendation 4.1), the establishment of a cybersecurity hygiene posture within the industry (Recommendation 4.2), industry education outreach and engagement (Recommendation 4.5), and patient education programs (Recommendation 4.6). *Id*. at 40-46.
5. **Identify and develop better mechanisms against cyberattacks and other exposures targeting research and development and intellectual property (Imperative 5).** The Task Force included recommendations for developing guidance on the value of R&D and the economic value if it is lost (Recommendation 5.1) and engaging in research to develop ways to better protect big data sets (Recommendation 5.2). *Id*. at 48-49.
6. **Improve information sharing of cyber threats and risks and mitigations strategies within the health care industry (Imperative 6).** The Task Force emphasized the importance of information sharing by public and private industry stakeholders and using a flexible approach to leverage the sharing initiatives currently in use. Recommendations include tailoring information sharing so it can be consumed more easily by smaller organizations that rely on limited or part-time security staff (Recommendation 6.1), HHS collaboration with industry and information sharing organizations to more effectively disseminate and utilize information (Recommendation 6.2), and encouraging annual readiness exercises by the health care industry (Recommendation 6.3). *Id*. at 50-53.

Further information about the Report and the Task Force's work can be found at HHS's blog, located here.

Issues on the Horizon

- **Reconciliation of Ohio's Biennium State Budget Underway.**

  On June 21, the Ohio Senate passed a $65.4-billion budget for the next two years. The Senate's budget made more than 150 changes to the version presented by the House. Now the chambers have until June 30 to reconcile their respective versions and present a final budget to Governor Kasich. Tucker Ellis's Health Care Practice Group is monitoring the status of the budget negotiations and will report any significant financial impacts on health care services.

- **Anticipated Decision in the Stewart "Apology Statute" Case.**

  On April 6, oral arguments were held in *Stewart v. Vivian* pending before the Ohio Supreme Court (Case No. 2016-1013). The Stewart case examines Ohio's "apology statute" and whether it bars statements of fault, error, or liability from admission into evidence when such statements are made during the course of apologizing or commiserating with a patient or a patient's family. The Court's decision is expected in the coming weeks. Stay tuned for future editions of *The Pulse* for any breaking developments in this case.

This newsletter has been prepared by Tucker Ellis LLP for the use of our clients. Although prepared by professionals, it should not be used as a substitute for legal counseling in specific situations. Readers should not act upon the information contained herein without professional guidance.