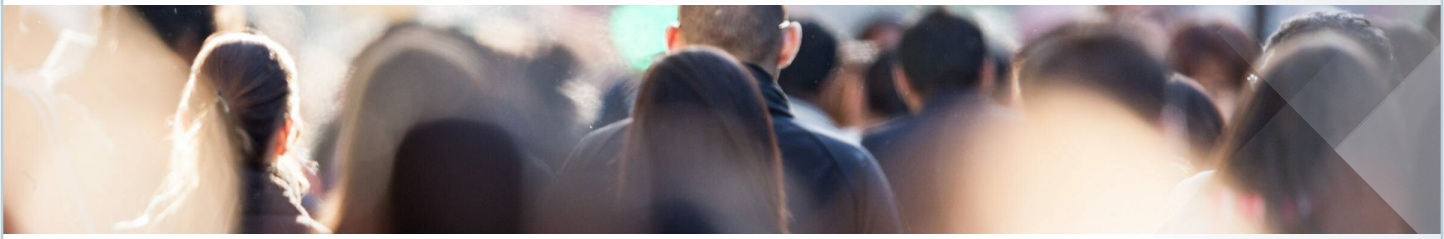
BURR FORMAN LLP



Hot Topics in Health Care July 2023

Article
07.26.2023

Progress of Pre-Submissions for Medical Devices Now Trackable Through CDRH Portal

Medical device manufacturers must submit applications for certain classes of medical devices for approval by the Food and Drug Administration ("FDA") prior to product development, marketing and sale through its Center for Devices and Radiological Health ("CDRH"). The FDA's Q-Submission Program provides medical device manufacturers with the opportunity to engage in discussions with FDA review teams during the product development process, obtaining early feedback from the agency on various premarket submissions. Pre-Submissions are the original and most common type of Q-Submission, affording manufacturers an opportunity to obtain the FDA's feedback on future premarket approval (PMA) applications, investigational device exemption (IDE) applications, premarket notification (510(k)) submissions, humanitarian device exemption (HDE) applications, and de novo reclassification requests. The FDA issued final guidance for its Q-Submissions Program in June 2023.

To facilitate the regulatory process, the FDA developed its CDRH Customer Collaboration Portal ("CDRH Portal") to allow users to track the progress of Pre-Submissions through its electronic Submission Template and Resource ("eSTAR"). The FDA issued final guidance on eStar for 510(k) premarket notification submissions in September 2022. On May 22, 2023, the FDA announced it had updated the CDRH Portal to allow users to track the progress of Pre-Submissions, issuing final guidance on June 2, 2023. Beginning October 1, 2023, all 510(k) submissions must be submitted as

RELATED PROFESSIONALS

Chester "Chet" J. Hosch

RELATED CAPABILITIES

Health Care

Health Care Business, Governance & Transactional

Health Care Compliance

Health Care Litigation

electronic submissions using eSTAR absent exemption.

Exceptions to Transition from COVID-19 EUAs, Policies for Medical Devices

With the expiration of the COVID-19 public health emergency on May 11, 2023, the Food and Drug Administration ("FDA") issued two guidance documents addressing medical devices that were subject to emergency use authorizations ("EUAs") to spur the availability of devices that could respond to the COVID-19 pandemic: --"Transition Plan for Medical Devices Issued Emergency Use Authorizations Related to Coronavirus Disease 2019 (COVID-19)" and "Transition Plan for Medical Devices That Fall Within Enforcement Policies Issued During the Coronavirus Disease 2019 (COVID-19) Public Health Emergency." These guidances are intended to help facilitate what the FDA called "an orderly and transparent transition" for these products from the temporary COVID-19-related measures to the agency's normal regulatory requirements.

During the COVID-19 public health emergency ("PHE"), the FDA issued almost 1,000 EUAs for devices to enable access to nearly 500 different devices used to help diagnose, treat or prevent the disease, including in vitro diagnostic tests, personal protective equipment, and ventilators. The agency also issued guidance documents setting the terms of enforcement policies that were intended to help expand the availability of some devices during the PHE, including ventilators, remote monitoring devices, surgical masks, and gloves. The FDA Center for Devices and Radiological Health ("CDRH") said that it is now "taking steps to assist stakeholders, including industry, health care professionals and patients, who many need time to transition from certain temporary emergency measures."

Despite the end of the PHE, the Department of Health and Human Services ("HHS") has determined it will extend EUAs issued by the FDA for:

- in vitro diagnostics for detection and/or diagnosis of SARS-CoV-2, the virus that causes COVID-19;
- personal respiratory protective devices;
- other medical devices, including alternative products used as medical devices; and
- drugs and biological products.

HHS determined these EUAs should not be immediately terminated because COVID-19 continues to present a significant potential for a public health emergency and to affect the health and security of citizens living abroad. Therefore, these EUAs at present remain in effect indefinitely.

OCR Provides Cybersecurity Reminders in Its June 2023 Newsletter

HIPAA covered entities and business associates ("Regulated Entities") are required to implement authentication solutions of sufficient strength to ensure the confidentiality, integrity, and availability of their Protected Health Information ("PHI"). In its most recent newsletter, the Office of Civil Rights ("OCR") provides helpful tips regarding the implementation of authentication solutions, consistent with its recent enforcement action against Banner Health resulting in a $1.25 million and corrective action settlement.

Hot Topics in Health Care July 2023

As a best practice, regulated entities should consider implementing multi-factor authentication solutions, including phishing-resistant multi-factor authentication, where appropriate to improve the security of ePHI and to best protect their information systems from cyber-attacks.

The HIPAA Security Rule requires Regulated Entities to implement authentication procedures "to verify that a person or entity seeking access to electronic protected health information is the one claimed." However, the HIPAA Security Rule does not impose any specific authentication solution.

In keeping with HIPAA Security Rule's design to be flexible, scalable, and technology neutral, the authentication standard does not prescribe the implementation of specific authentication solutions. Instead, a regulated entity's risk analysis should inform its selection and implementation of authentication solutions that sufficiently reduce the risks to the confidentiality, integrity, and availability of ePHI. Different touchpoints for authentication throughout a regulated entity's organization may present different levels of risk, thus requiring the implementation of authentication solutions appropriate to sufficiently reduce risk at those various touchpoints.

Even after a regulated entity implements authentication procedures, its obligations do not end. To ensure such procedures continue to provide reasonable and appropriate protection of PHI, Regulated Entities must maintain an ongoing obligation to review and modify the security measures implemented under the Security Rule.

OIG Issues Final Rule for Blocking Penalties

On June 27, 2023, the Office of Inspector General ("OIG") for the Department of Health and Human Services ("HHS") posted its final rule implementing information blocking penalties for enforcement beginning September 1, 2023. The final rule does not impose new information blocking requirements. OIG incorporated regulations published by the Office of the National Coordinator for Health Information Technology ("ONC") as the basis for enforcing information blocking penalties. Instead, the final rule establishes the statutory civil money penalties created by the 21st Century Cures Act ("Cures Act") amending the Public Health Service Act ("PHSA") of up to $1 million if OIG determines an individual or entity has committed information blocking.

Information blocking is a practice by an "actor" that is likely to interfere with the access, exchange, or use of electronic health information ("EHI"), except as required by law or specified in an information blocking exception.

Penalties are assessed based upon knowledge standards set forth in the Cures Act. For healthcare providers, the law applies the standard of whether the providers know that the practice is unreasonable and is likely to interfere with the access, exchange, or use of EHI. For developers of certified health information technology ("IT"), health information exchanges ("HIE"), and health information network ("HIN"), the law applies the standard of whether they know, or should know, that a practice is likely to interfere with the access, exchange, or use of EHI.

Hot Topics in Health Care July 2023

CMS Announces Temporary Gap in Competitive Bidding Program for Durable Medical Equipment

The Centers for Medicare & Medicaid Services ("CMS") announced a temporary gap in the Durable Medical Equipment, Prosthetics, Orthotics & Supplies ("DMEPOS") Competitive Bidding Program ("CBP") for off the shelf back and knee braces starting on January 1, 2024. During this gap, Medicare payment will generally continue at current payment allowances established through competitive bidding, adjusted by inflation, and following payment provisions in statute and regulation. CMS will seek to establish sustainable prices for durable medical equipment, prosthetics, orthotics, and supplies, through rulemaking, saving money for Medicare enrollees and taxpayers without risking access to quality equipment in the Medicare program. As always, its efforts are intended to limit fraud, waste, and abuse in the Medicare program. CMS will resume bidding after receiving public comment through rulemaking.

The DMEPOS CBP was authorized by Congress in the Medicare Prescription Drug, Improvement, and Modernization Act of 2003. The statute requires Medicare to replace the current fee schedule payment methodology for selected DMEPOS items with a competitive bid process to improve the effectiveness of the Medicare methodology for setting DMEPOS payment amounts. Under the program, a competition among suppliers who operate in a particular competitive bidding area is conducted. Suppliers are required to submit a bid for selected products electronically through a web-based application process. Bids are evaluated based on the supplier's eligibility, financial stability and bid price, with contracts awarded to the Medicare suppliers meeting these standards. Contract suppliers must agree to accept assignment on all claims for bid items and will be paid the single payment amount.

During the temporary gap, Medicare payment will generally continue at current payment allowances established through competitive bidding, adjusted by inflation, and following payment provisions in statute and regulation. Information can be found in this fact sheet. DME providers are encouraged to monitor the CMS website and the Competitive Bidding Implementation Contractor ("CBIC") website for updates.

New Web Pages to Help Consumers Understand Rights and Protections Under No Surprises Act

To help consumers understand their rights and protections under the No Surprises Act, CMS created a new set of web pages on CMS.gov, providing consumer content. In addition to providing information about protection against unexpected medical bills, the pages include an interactive tool to help consumers identify actions they can take to resolve their billing situation, as well as a redesigned complaint form so they can more easily report a violation if they believe the rules aren't being followed.

In July 2021, the U.S. Departments of Health and Human Services ("HHS") released the "Requirements Related to Surprise Billing; Part I," to restrict surprise billing for patients in job-based and individual health plans who get emergency care, non-emergency care from out-of-network providers at in-network facilities, and air ambulance services from out-of-network providers. In October 2021, HHS released the "Requirements Related to Surprise Billing; Part II," which provides additional protections against surprise medical bills, including:

- Establishing an independent dispute resolution process to determine out-of-network payment amounts between providers (including air ambulance providers) or facilities and health plans.

- Requiring good-faith estimates of medical items or services for uninsured (or self-paying) individuals.
- Establishing a patient-provider dispute resolution process for uninsured (or self-paying) individuals to determine payment amounts due to a provider or facility under certain circumstances.
- Providing a way to appeal certain health plan decisions.

In November 2021, the "Prescription Drug and Health Care Spending" interim final rule was issued, implementing new requirements for group health plans and issuers to submit certain information about prescription drug and health care spending. This includes, among other things, information on the most frequently dispensed and costliest drugs, and enrollment and premium information, including average monthly premiums paid by employees versus employers.

In August 2022, HHS issued final rules titled "Requirements Related to Surprise Billing: Final Rules." The rules finalize requirements under interim final rules relating to information that group health plans and health insurance issuers offering group or individual health insurance coverage must share about the qualifying payment amount ("QPA"). Together, these rules lay the groundwork to provide consumers with protection against surprise billing. Consumers can learn more about policies, resources, payment resolution and advocates through the No Surprise Act website maintained by CMS. The federal and state courts continue to address these final rules.

FDA Postpones Enforcement of New Premarket Cyber Requirements

Under final guidance from the Food and Drug Administration ("FDA"), medical device manufacturers subject to cybersecurity vulnerabilities will now have until October 1, 2023 to comply with recently enacted premarket submission requirements for their devices under the Food and Drug Omnibus Reform Act of 2022 ("FDORA"). By that date, the FDA said device sponsors "will have had sufficient time to prepare premarket submissions that contain information required by [FDORA]."

The guidance, "Cybersecurity in Medical Devices: Refuse To Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act," advises the FDA will not issue refuse-to-accept ("RTA") decisions for premarket submissions that the FDA receives regarding so-called cyber devices if the submissions do not provide the information required for such submissions under FDORA. Instead, the agency will "work collaboratively with sponsors of such premarket submissions as part of the interactive and/or deficiency review process." Under FDORA, the effective date for these requirements was originally June 27, 2023.

Under FDORA enacted in December 2022, medical device manufacturers submitting premarket submissions (i.e., 510(k) premarket notifications, de novo classification requests, premarket approval ("PMA") applications, product development protocols, or requests for a humanitarian device exemption) for cyber devices must submit "such information as the [FDA] may require" to ensure that the product meets cybersecurity requirements specified by FDORA. As defined in FDORA a "cyber device" is a device that: (i) includes software validated, installed or authorized by the sponsor "as a device or in a device"; (ii) can connect to the internet; and (iii) contains technological characteristics validated, installed or authorized by the sponsor that could be vulnerable to cybersecurity threats.

The new submission requirements specified in FDORA for cyber devices include the following:

- *Cybersecurity vulnerability monitoring*. The sponsor must submit a plan to monitor, identify and address "as appropriate, in a reasonable time," postmarket cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures.
- *Cybersecurity assurance processes*. The sponsor must design, develop and maintain processes and procedures to provide a reasonable assurance that the device and related systems are "cybersecure" (i. e., the processes and procedures must address known unacceptable vulnerabilities "on a reasonably justified regular cycle" and critical vulnerabilities that could cause uncontrolled risks outside the regular cycle of addressing known vulnerabilities "as soon as possible"
- *Software bill of materials*. The sponsor must provide the FDA a software bill of materials, including the commercial, open-source and off-the-shelf software components of the device.

FDORA authorizes the FDA to require compliance with other requirements that the agency may establish through regulation "to demonstrate reasonable assurance that the device and related systems are secure."

Georgia DHS Announces Opening of Grant

The Georgia Department of Human Services ("DHS") announced on July 11, 2023 the opening of the 2023 State of Hope grant cycle. The announcement invites organizations and individuals to apply for funding for projects that will "keep children safe, strengthen families, and empower communities." The deadline for submission is August 11, 2023.

The State of Hope grant prioritizes education, trauma awareness, quality caregiving and economic self-sufficiency. These are areas DHS believes will have "the greatest impact in supporting healthy families and building family protective factors to keep children safe within their families." This year, priority consideration will be given to proposals promoting one or more of Georgia's Objectives for Prevention:

- economic stability
- mental and physical health
- increased access to early childhood education
- increased knowledge of child abuse and neglect prevention

Through this grant cycle, DHS seeks to empower and equip Georgians in developing these initiatives. DHS invites all interested parties to "take advantage of this grant opportunity and contribute to the self-sufficiency, safety, and well-being of Georgia's children and families."

Applicants are requested to submit complete applications via the portal located at dfcs.georgia.gov/about-us/state-hope. Detailed guidelines and application requirements are available on that webpage.