KING & SPALDING

Client Alert

FEBRUARY 8, 2022

For more information, contact:

Eric Henry
+1 302 312 9772
ehenry@kslaw.com

Lisa M. Dwyer
+1 202 626 2393
ldwyer@kslaw.com

Jessica Ringel
+1 202 626 9259
jringel@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006
Tel: +1 202 737 0500

San Francisco
50 California Street
San Francisco, CA 94111
Tel: +1 415 318 1200

Chicago
110 N Wacker Drive
Chicago, IL 60606
Tel: +1 312 995 6333

New Standard Maps Medical Device Software Development Standard to Health Software and Health IT Cybersecurity

The International Electrotechnical Commission (IEC) and the International Organization for Standards (ISO) recently published a cybersecurity standard that has received limited press but may have a significant impact on device and non-device health software companies. The standard was released as IEC 81001-5-1:2021, and it is the first in what is expected to be a series of IEC 81001 health software standards.

The scope of the standard is:

- Software in a Medical Device (SiMD);
- Software as part of hardware specifically intended for health-related use;
- Software as a medical device (SaMD); and
- Software-only products for other health-related uses.

The most significant feature of the new standard is that it uses the IEC 62304:2006 +AMD1:2015 (Medical device software – software life cycle processes) standard as the basis for its activities and deliverables, and it embeds cybersecurity requirements into each IEC 62304 process step. Although ubiquitous among medical device manufacturers, the IEC 62304 standard may impose a set of lifecycle activities on non-device health software companies that the companies may not have previously considered.

Although Annex A to IEC 81001-5-1:2021 states that following IEC 62304 is not a requirement for compliance with IEC 81001-5-1:2021, in our view (and implied by the language of the Annex) compliance with IEC 81001-5-1 may be problematic without also aligning with the IEC 62304 standard (e.g., requirements regarding Software of Unknown Provenance (SOUP), software architectural design, safety risk management, problem resolution, and documented static reviews of requirements, architecture, and design).

Other notable provisions in the new standard include the following:

- New Risk Considerations – Although correlated with safety risk management, risk in this standard addresses cybersecurity vulnerabilities and threats beyond those impacting safety. This is consistent with cybersecurity guidance from a variety of sources (e.g., Association for the Advancement of Medical Instrumentation (AAMI) and the National Institute for Standards and Technology (NIST) in the U.S., the Medical Device Consortium Group (MDGC) in the EU, and Health Canada). It is, however, inconsistent with current U.S. Food and Drug Administration (FDA) cybersecurity guidance, which limits consideration of cybersecurity risk to safety-related issues.

- Threat Modeling – The emphasis on threat modeling is consistent with that of the FDA and others, and the standard incorporates threat modelling into its discussion of the "Security Risk Management Process" in Sections 4.2, 7, and B.3. Threat modeling is discussed in depth in Annex C, where the standard identifies several acceptable approaches. We also note that the standard directs manufacturers to avoid the trap of simplistic mitigations to threats and to instead adopt a defense-in-depth architecture.

- Training and Assessment Programs – Section 4.1.4 of the standard requires manufacturers to identify and provide security training and assessment programs, which aligns broadly with the personnel sections of both U.S. medical device regulations and the ISO 13485:2016 medical device quality system standard. The requirement, however, goes beyond many other global cybersecurity guidance documents in this respect.

- New Software Classification – Whereas the IEC 62304 medical device software lifecycle standard classifies software systems based on the severity of pre-mitigated safety risks, IEC 81001-5-1 is applicable across all safety classes and instead classifies software based on the ownership of cybersecurity risk (i.e., "risk transfer"). The risk transfer categories are "maintained," "supported," or "required." The responsibilities of the manufacturer for each of these classes is elaborated in Annex A.3.

- Software System Verification – Testing at the software system level (section 5.7 of the new standard) requires testing of not only security requirements within overall software system requirements but also of threat mitigations from the threat model, vulnerability testing, and penetration testing. For organizations that have not made threat models the center of their cybersecurity risk management and design verification planning, these requirements likely represent a significant change to current practices.

- Conflicts of Interest – Section 5.7.5 of the standard emphasizes managing conflicts of interest between testers and developers for a series of six design verification test types. We see the production of objective evidence of compliance to this requirement as a potential challenge to especially small software development companies.

- Software Bills of Material – The recent emphasis placed on Software Bills of Material (SBOMs) by FDA is lacking within this standard although they are mentioned in a note to Annex E acknowledging SBOMs as a requirement of IEC 60601-4-5.

- Monitoring Vulnerabilities/Verifying Security Updates – There is significant real estate in the maintenance section of the standard (Section 6) dedicated to monitoring for vulnerabilities and the verification and release of security updates. Vulnerability disclosure (consistent with most other global guidance documents) is correspondingly integrated as a requirement in Section 4.1.7.

- Legacy Software – Similar to the IEC 62304 provision for legacy software introduced in the 2015 update, IEC 81001-5-1 dedicates Annex F to "Transitional Health Software" and provides steps for building cybersecurity confidence in systems not developed in compliance with the standard.

King & Spalding will be watching how the FDA reacts to the release of this standard in two respects: (1) how IEC 81001-5-1 harmonizes (or does not harmonize) with the second draft of FDA's premarket cybersecurity guidance due this year and (2) if and when FDA incorporates IEC 81001-5-1 into its list of recognized consensus standards. The firm will also monitor potential changes to existing cybersecurity guidance from MDCG, Health Canada, Australia's TGA, and the International Medical Device Regulator's Forum (IMDRF). Within the EU in particular, there is a potential that IEC 81005-5-1 may be classified as a harmonized standard to the EU's Medical Device Regulation (EU MDR) in the future.

We encourage companies across the health software spectrum to obtain a copy of this standard and clearly understand any gaps with current practices.

King & Spalding LLP regularly counsels health software and medical device companies on cybersecurity issues and compliance with applicable global regulations and standards in the life sciences. Please let us know if we can be of any assistance in navigating the rapidly changing cybersecurity and health software landscape.

ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,200 lawyers in 22 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

This alert provides a general summary of recent legal developments. It is not intended to be and should not be relied upon as legal advice. In some jurisdictions, this may be considered “Attorney Advertising.” View our Privacy Notice.

ABU DHABI
ATLANTA
AUSTIN
BRUSSELS
CHARLOTTE
CHICAGO
DUBAI
FRANKFURT
GENEVA
HOUSTON
LONDON
LOS ANGELES
MOSCOW
NEW YORK
NORTHERN VIRGINIA
PARIS
RIYADH
SAN FRANCISCO
SILICON VALLEY
SINGAPORE
TOKYO
WASHINGTON, D.C.