Elektronisches Patientendossier Die Zertifizierung EPDG-TOZ

Healthcare Newsletter Februar 2019

Auf der Basis des Bundesgesetzes über das elektronische Patientendossier (EPDG) wird die Schweiz ab 2020 einen systematischen Austausch von elektronischen Patientendaten einführen. Dabei wird nicht ein schweizweit zentralisiertes System vorgesehen, sondern es wurde bewusst ein eigenverantwortlicher Zugang gewählt. Institutionen des Gesundheitswesens schliessen sich hierzu (Stamm-)Gemeinschaften an oder gründen solche selbst. Der Datenaustausch findet danach in einem standardisierten Format zwischen den einzelnen Systemteilnehmern statt.

Die Herausforderung
Gemäss der im EPDG formulierten rechtlichen Voraussetzungen sind durch die Systemteilnehmer technische und organisatorische Zertifizierungsvoraussetzungen (TOZ) zu erfüllen. Um am elektronischen Datenaustausch teilnehmen zu können, ist die Einhaltung dieser Mindeststandards mittels einer Zertifizierung zwingend nachzuweisen. Hierbei ist insbesondere der Grundsatz zu beachten, dass nicht die System-/ Plattformanbieter zertifiziert werden, sondern die Institutionen, welche die jeweiligen Systeme benutzen bzw. Schnittstellen in ihre eigenen Systemlandschaften integrieren und in diesen betreiben. Die technischen Kontrollanforderungen bei den Plattform-Providern für e-Patientendossiers werden aber in einem separaten Assessment evaluiert.

Unsere Leistung
Basierend auf den ISO-Akkreditierungsbestimmungen zur Zertifizierung von Produkten, Prozessen und Dienstleistungen (ISO/ IEC 17065) sowie für Managementsysteme (ISO/ IEC 17021-1) hat KPMG ein vollständiges Prüfprogramm für die Zertifizierung von EPDV-EDI Anhang 2 (TOZ) und EPDV-EDO (IDP) Anhang 8 erarbeitet. Dieses umfasst im Wesentlichen die prozessualen, strukturellen und operativen softwaresystemtechnischen Anforderungen im Zusammenhang mit dem Betrieb der EPDs. Zusätzlich bietet KPMG eine Zertifizierung für Anbieter von Identifikationskarten (z.B. Krankenkassen- und/ oder Ärztekarten etc.) im Gesundheitswesen an. Dabei geht es um einen detaillierten Nachweis der Funktionsfähigkeit und Sicherheit der verwendeten Technologien sowie der Produktions- und Lieferprozesse für die Aushändigung von Patienten-Identifikationskarten.

Unser Vorgehen
Im Rahmen eines Gap/ Maturity Assessment wird im Vorfeld des eigentlichen Audits eine Beurteilung der Ist-Situation durchgeführt. Diese erlaubt wesentliche offene Punkte zu erkennen und kann auch unabhängig von einem späteren Audit zwecks Standortbestimmung durchgeführt werden. Die Durchführung des Audits gliedert sich anschliessend in drei Phasen (Vorphase, Dokumentationsaudit, Implementation Audit). Als Ergebnis erhalten Sie einen strukturierten Zertifizierungsbericht, in welchem Feststellungen und Beobachtungen zu jeder geforderten Kontrolle festgehalten sowie Empfehlungen zu möglichen Nichtkonformitäten gegeben werden. Diese sind innerhalb von sechs Monaten umzusetzen, um ein definitives eidgenössisches Zertifikat zu erhalten. In den Folgejahren sind zwei «Wiederholungsaudits» durchzuführen, welche gezielt Teilaspekte (z.B. Veränderungen in der Systemlandschaft oder bei Schnittstellen) prüfen. Im darauf folgenden vierten Jahr ist eine vollumfängliche Re-Zertifizierung nachzuweisen. Aufgrund der hohen Vernetzung der Systemteilnehmer untereinander sind einheitliche Prozesse und Sicherheitsstandards innerhalb des EPD-Systems von grosser Bedeutung. Um diesem Anspruch nachzukommen, ist das Prüfprogramm umfassend gestaltet und kann grob in drei Themenfelder gegliedert werden: Der Bereich «Prozesse und Organisation» befasst sich schwerpunktmässig mit der Dokumentation von Weisungen und Arbeitsvorgängen sowie Prozessabläufen inkl. der Verantwortlichkeiten in der IT-Organisation Ihrer Einrichtung. Im Bereich «IT, Betrieb und Wartung» werden die notwendigen Anforderungen des EPDV-EDI Anhang 2 (TOZ) an das Umfeld des technischen EPD-Systems, z.B. ERP-

Anwendungen, Identifikationsprozesse, Zugangsrechte, Integritätsanforderungen sowie weitere technische Info.-Sec.-Sicherheits- und Umweltanforderungen abgedeckt. «Software Script Testing» seinerseits beinhaltet ein Schwergewicht einer Vielzahl von Kontrollen innerhalb der Applikationen, der Plattformarchitektur, der Betriebssysteme, der Datenbanken sowie hinsichtlich der Konfiguration der Zugänge und der Verschlüsselungen der Datensätze bis zur Archivierung von Patientendossiers. Das Software-Testing stellt sicher, dass das EPD-System, auf Basis der Integrität, Härtung der IT-Systeme und der Vertraulichkeit, den höchsten Ansprüchen im Bereich des Datenschutzes und der Informationssicherheit auf logischer/technischer Ebene gesichert wird.

Kontakt

KPMG AG
Badenerstrasse 172
Postfach
CH-8036 Zürich

kpmg.ch

Michael Herzog
Partner
Government & Healthcare

+41 58 249 40 68
michaelherzog@kpmg.com

Reto Grubenmann
Director, Leiter
Zertifizierungsstellen

+41 58 249 42 46
retogrubenmann@kpmg.com