## CYBERSCHUTZ – Sensibilisierung im Gesundheitswesen

# QM als Waffe gegen Cyber-Crime

HÄUFIG GESTELLTE FRAGEN UND ANTWORTEN IM GESUNDHEITSWESEN

**Expertenfrage an Mark Peters**

Die DSGVO ist in Kraft. Inwiefern fallen die Themen Cyber-Sicherheit also in den Bereich Datenschutz? Wie integriere ich die geforderte Informationssicherheit in mein QM-System?

Cyber-Angriffe und Cyber-Sicherheit werden derzeit intensiv in der Öffentlichkeit diskutiert. Für Hersteller, Dienstleister und Anwender von Informationstechnik stellen sich in diesem Zusammenhang viele Fragen, insbesondere hinsichtlich der Betroffenheit des eigenen Verantwortungsbereichs. Das vorliegende Dokument greift die wichtigsten und häufigsten Fragen zur Cyber-Sicherheit auf und vermittelt anhand der Antworten einen schnellen Einstieg in das Thema.
**Schulungen unter:** www.bublitzpeters.de/akademie

DATENSCHUTZEXPERTE MARK PETERS GIBT DAZU ANTWORTEN:

### E-Rezepte, App, Konnektor

Der digitale Umbruch ist in vollem Gange – und es gibt kein Unternehmen im Gesundheitswesen, das nicht in irgendeiner Form personenbezogene Daten verarbeitet. Datenschutz ist damit ein entscheidender rechtlicher Qualitäts- und Sicherheitsaspekt.

MARK PETERS
BSI-Grundschutz-Praktiker
QM-Auditor im Gesundheitswesen

**Fragen an:**
info@
bublitz-peters.de

**Praxismanagement**
**Bublitz-Peters GmbH & Co. KG**
Rohrbacher Straße 28
69115 Heidelberg

### ISO, KTQ, QEP und Heidelberger Datenschutz-Rating

Mit der Revision der ISO 9001 von 2017 kann der Datenschutz in Kapitel 4, dem „Kontext der Organisation“, und dabei insbesondere unter dem Punkt 4.4 „Qualitätsmanagement und dessen Prozesse“ setzen. Datenerhebung und -verarbeitung sind ein Bestandteil der Praxis beziehungsweise deren Prozesse und haben Auswirkungen auf die Qualität und Sicherheit in der Therapie. Deshalb müssen resultierende Risiken auch im Qualitätsmanagement-Cyberschutz oder Datenschutzmanagementsystem umgesetzt werden.

Die Übersicht über den Ablauf Datenerhebung und -verarbeitung hat der Datenschutz-beauftragte (DSB) beziehungsweise der Cyberschutzkoordinator.

### Know-how verbinden

Auch unter Punkt 7 „Unterstützung“ kann Datenschutz als Teil des QM-Systems betrachtet werden; damit müssen dem DSB ausreichend Ressourcen (Zeit, Know-how Geld ...) zur Verfügung stehen, damit er seine Aufgaben vollständig erfüllen kann. Abhängig von der Praxisgröße, aber auch weitere Mitarbeiter, die ihn zum Beispiel als Koordinatoren unterstützen. Kapitel 7.1.5. fordert eine zuverlässige Überwachungs- und Messtechnik, also für den DSB beispielsweise ein geeignetes Cyberschutz-Tool für das Management von Cyberschutzanforderungen; Kapitel 7.4. sieht Kommunikation als wichtigen Teil des QMS vor – zum Beispiel betrifft das den Umgang mit Datenschutzverletzungen.

**IT & Cyberschutz**

Im Rahmen der Sicherung der Qualität im Betrieb gemäß Kapitel 8 der Norm ist abzuklären, ob der Datenschutz bei der Entwicklung, etwa von IT-Dienstleistungen, einbezogen werden muss. Besonders bei Dienstleistungen von EDV-Lieferanten gilt es, die Datenschutzrelevanz abzuklopfen – zum Beispiel bei der externen Auftragsdatenverarbeitung. In diesen Rahmen muss auf die neuen KBV- und BSI-IT-Richtlinien geachtet werden. (Ärzteblatt 05.11.2019)

**QM – Methoden**

Datenschutzbeauftragte profitieren von einem Blick auf die Methoden der QM-Systeme (KTQ, QEP, ISO 9001). Beispielsweise ist es für den DSB notwendig, seinen Zuständigkeitsbereich klar zu definieren – ISO 9001 Normenkapitel 4.3. Der DSB kann sich an Punkt 5 der QM-Norm orientieren und die Geschäftsleitung zur Unterstützung im Bereich Datenschutz auffordern. Mit der Lenkung dokumentierter Information in Kapitel 7.5.3. entwickelt der DSB eine strukturierte Ablage.

**PDCA/Dokumentation**

Gibt es Nichtkonformitäten, fordert das Normenkapitel 8.7. Lenkungsprozesse und Korrekturmaßnahmen. Diese Vorgabe ist für den Datenschutz beziehungsweise nach Verletzungen nötig. Zum Beispiel nach einem Cyber-Angriff (erfolgreich oder nicht) muss die getroffene Maßnahme auch auf Wirksamkeit überprüft werden (KVP).

**Weiterbildungen**

Den für das QM-System vorgeschriebenen kontinuierlichen Verbesserungsprozess sollten DSB ebenfalls für ihren Bereich übernehmen. Dafür sollte auch der Datenschutz regelmäßig per internen Daten und IT-BSI-Audit unter die Lupe genommen und optimiert werden. Der DSB und Cyberschutz Koordinator sollten als interne Auditoren fungieren.
Die passende Weiterbildung gibt es beispielsweise in der Praxismanagement Bublitz-Peters Akademie: www.bublitzpeters.de/akademie/

**PDCA**

Am Ende steht ein Abschlussreport (Review-Report), der sich eignet, um den Arzt, die Pflegeleitung oder GF zu informieren. Abschließend lassen sich die nächsten Verbesserungsschritte beschließen (PDCA).

**Menscheln mit TOM**

Grundsätzlich bietet es sich an, den Datenschutzbeauftragten (DSB) auch externen DSB und den Qualitätsmanagementbeauftragten (QMB) zusammenzubringen, damit sie gegenseitig vom Know-how des anderen profitieren: Beispielsweise technische Maßnahmen (TOM) sind das „A und O“, da Arztpraxen immer öfter Opfer von Cyberangriffen werden.
Quelle: BSI, ZAC 2019

Dem QMB fehlt es oft an Verständnis für die Bedeutung des Bereichs Cyber- und Datenschutz als Qualitätsaspekt. Die DSBs profitieren vom methodischen Ansatz eines Qualitätsmanagementsystems, das sich auf den eigenen Bereich als Datenschutzmanagementsystem übertragen lässt. Im Sinne eines kontinuierlichen Austauschs.
Insgesamt stärkt QM-Systeme wie QEP, KTQ oder die neue ISO 9001 die Stellung des DSB in Kliniken, Pflegeheimen oder Arztpraxen und gibt dem Datenschutz mehr Raum als notwendigen Bestandteil des Qualitätsmanagements.

**Heidelberger Datenschutz-Rating mit Zertifizierung HDR**

Durch das HDR wird der Daten- Cyberschutz für alle Beteiligten transparent. Das stärkt vor allem Vertrauen. So wissen die Patienten und Angehörigen, dass ihre Daten in sicheren Händen sind. Das Zertifikat führt darüber hinaus zu einem positiven Behörden- und Öffentlichkeitsbild.
www.datenschutzzertifizierung.info

**Bundesrat billigt neue Benennungsgrenze für Datenschutzbeauftragte**

Das Gesetz wurde im Gesetzesblatt veröffentlicht. Es ist somit seit dem 25.11.2019 geltend.
Infos unter:
www.baden-wuerttemberg.datenschutz.de/faq-datenschutz-in-der-arztpraxis/

**Neu**

Heidelberger Cyberschutz-Rating:
www.cyberschutzzertifizierung.de