VA Notfallmanagement im Rahmen der IT-Sicherheitsrichtlinie

Übersicht

Die IT-Sicherheitsrichtlinie nach § 75c SGB V regelt technische und organisatorische Maßnahmen (TOM) für medizinische Versorgungseinrichtungen wie Krankenhäuser und Kliniken zum Schutz vor Schadensfälle in der IT-Anwendung.

Ziel und Zweck

Die Verfahrensanweisung hat das Ziel, die Abläufe und allgemeinen Regelungen zum Notfallmanagement in der IT-Sicherheit in strukturierten Prozessen und Verfahren transparent umzusetzen und gut verständlich darzustellen. Ziel dieser Beschreibung ist die Vereinheitlichung der Abläufe und die Sicherstellung des Prozesses, der geregelt wird und die Gewährleistung der Vollständigkeit sowie der geplanten Ergebnisqualität.
Die Informationstechnologie ist heute wesentlicher Bestandteil einer Klinik und von Krankenhäusern. Es werden wesentliche sicherheitsrelevante Informationen zu den Patientenfällen gespeichert. Fällt das IT-Netzwerk aus so können beispielsweise die Notfalldaten von Patienten fehlen und zu falschen Diagnose- und Therapieentscheidungen führen.
Ziel dieser VA ist deshalb die transparente Regelung für Notfälle in der IT-Sicherheit.

Anwendungsbereich

Diese Anweisung gilt für alle Bereiche der Einrichtung.

Der Anwendungsbereich ist unabhängig von den Standorten der Einheiten und ist definiert für alle Bereiche, in denen IT-Systeme eingesetzt und personenbezogene Daten, erfasst, verarbeitet, übertragen und gespeichert werden.

Verantwortung

Verantwortlich für die einzelnen Segmente des Verfahrens sind dazu beauftragte Personen, insbesondere:

- Leitung/Mitglieder der Leitung (ärztlich und organisatorisch)
- Informationssicherheitsbeauftragte (ISB)
- Datenschutzbeauftragte (DSB) und Datenschutzkoordinatoren (DSK)
- Externe Dienstleister, soweit rechtlich geregelt (Externe Datenschutzbeauftragte (DSB)

Die individuellen Verantwortungsbereiche sind in Protokollen, falls vorgesehen, zu dokumentieren.

Prozesse

Zur Gewährleistung der Patientensicherheit muss ein professionelles Notfallmanagement in jeder medizinischen Versorgungseinrichtung etabliert sein. Die Verpflichtungen für die Notfallversorgung sind in verschiedenen Gesetzen, Verordnungen und Richtlinien dokumentiert. Dazu gehört das Infektionsschutzgesetz, die Medizinprodukte-Regelungen, Hygienemanagement und auch Richtlinien für die IT-Sicherheit. Fällt das IT-Netzwerk aus, so stehen bei Einsatz der elektronischen Patientenakte auch keine umfassenden Notfallinformationen zu den einzelnen Patienten zur Verfügung.

Zu dem IT-Notfallmanagement gehört im ersten Schritt die Definition und Beschreibung eines IT-Notfalls. Diese Festlegungen hängen von der einzelnen Klinik und dem Computerisierungsgrad ab. So kann definiert werden, dass ein Notfall dann vorliegt, wenn für die Patientenversorgung wichtige Arbeitsplätze für einen längeren Zeitraum (z.B. länger als 15 Minuten) ausfallen. Für diesen Fall müssen Notfallpläne vorliegen, z.B. für unterbrochene oder abgebrochene Untersuchungen oder Therapien.

Konkrete Fragestellung: Wurde überprüft, ob es sich um einen tatsächlichen IT-Notfall handelt, erfolgt die Meldung an den oder die IT-Verantwortlichen? Dies erfolgt im Regelfall über ein Mobiltelefon, das immer unabhängig vom Computer- und Stromnetzwerk funktionieren muss. Dazu müssen die Notfallnummern wie auch die Telefonnummern der Feuerwehr, des Notarztes und der Polizei bekannt und deutlich sichtbar ausgehängt sein.

Für die praktische Nothilfe muss ein Aushang vorhanden sein, der den IT-Notfallbeauftragten und seine Telefonnummer enthält. Weiterhin müssen Verfahrensanweisungen oder interne Regelungen im Rahmen des Qualitätsmanagements vorliegen.

Danach sind die verschiedenen IT-Notfälle zu klassifizieren:

- Ausfall eines einzelnen IT-Arbeitsplatzes
- Ausfall aller IT-Arbeitsplätze einer Abteilung
- Ausfall des gesamten IT-Netzwerks

Im Rahmen des Qualitätsmanagements gibt es Checklisten und Verfahrensanweisungen / interne Regelungen für die möglichen Schweregrade eines IT-Notfalls.

Aktualisierung: nach 12 Monaten

Mitgeltende Dokumente:

- IT-Sicherheitsrichtlinie nach § 75b & 75c SGB V
- Bundesdatenschutz Gesetz (BDSG) Auszug § 64
- Datenschutz Grundverordnung (DSGVO) Auszug Art. 32

- § 135ff SGB V QM Richtlinie des GBA (GBA-RI)
- DKG-Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus (B3S)
- IT-Sicherheitsregelungen der Trägerschaften (z.B. RKD, EKD)
- BSI Grundschutz/VdS 10000 Standard
- Leitlinie zur IT-Sicherheit