Inhalt

1 Zweck und Anwendungsbereich

Dieses Dokument regelt die Vorgehensweise für die Implementierung und regelmäßige Überwachung eines Datenschutz- und Informationssicherheitssystems für die Mageretner-Tagesklinik. Um das Sicherheitsniveau möglichst hochzuhalten, ist es nötig sich an dieses Dokument zu halten und den internen Regelungen bei der Durchführung des Projekts Folge zu leisten.

2 Geltungsbereich

Diese Verfahrensanweisung betrifft nur die Mitarbeiter der Firma ISMED, die an dem Projekt beteiligt sind. Daraus erschließt sich, dass das Dokument laut TLP gelb ist, und somit die Weitergabe des Empfängers nur an die ausgewählten Mitarbeiter erfolgt.

3 Grundlagen

Da das Projekt im gesundheitlichen Sektor angesiedelt ist und es um den Schutz von Patientendaten geht, ist es wichtig, dass hierbei die DSGVO sowie das NISG in Kraft tritt. Es wird verlangt das Sicherheitskonzept für die Praxis nach aktuellen Standards und unter Einhaltung von entsprechenden Normen zu implementieren, um das Sicherheitsniveau im IKT-Bereich möglichst hochzuhalten.

CIA-Triade: Schutzziele der IT, anhand die Sicherheit in IKT-Systemen gemessen werden kann. Da sich das Projekt im IKT-Bereich befindet müssen diese Schutzziele möglichst zur Gänze erfüllt werden, um Gefahren bzw. Bedrohungen auszuschließen.

Vertraulichkeit: Schutz vor unbefugtem Zugriff auf Patientendaten

Verfügbarkeit: Schutz und Aufrechterhaltung der Services mit der höchsten Priorität (Diagnostik, Therapie)

Integrität: Schutz vor unbefugte Manipulation von Patienten oder medizinischen Daten

4 Vorgehensweise Informationssicherheitskonzept

Um die Schutzziele zu erfüllen, muss zunächst eine Prozessübersicht vorliegen, die gemeinsam mit dem Leiter der Praxis erarbeitet wird. Wenn alle Prozesse vorliegen, wird eine Kritikalitätsanalyse durchgeführt. Dabei wird definiert, welche Prozesse für die Praxis am wichtigsten sind und welche im Notfall eher vernachlässigt werden könnten. Um dies abzuschätzen befragt man den Leiter und überlegt für jeden Prozess, wie sich ein Stör- oder Ausfall auswirken würde (auf Patienten, sowie wirtschaftlich). Anschließend werden die Prozesse je nach Kritikalität priorisiert (gold= sehr kritikal, silber =kritikal, bronze = nicht kritikal). Danach wird überlegt welche Prozesse für die CIA-Triade von Bedeutung ist. Zu jedem von der CIA-Triade betroffenen Prozess werden die Risiken überlegt, die aus einem vordefiniertem Risikokatalog stammen, und inwiefern diese auf den Prozess wirken. Dabei stuft man diese anhand einer z.B. FMEA (Failure Mode and Effects Analysis) ein. Diese Risiken werden für jeden einzelnen Prozess in einer Risikomatrix platziert und so liegt vor welche Maßnahmen gesetzt werden müssen. Die Einstufung der Risiken richtet sich nach der Eintrittswahrscheinlichkeit und dem Schweregrad bei Eintritt. Risiken, die keine großen Auswirkungen haben werden grün markiert, Risiken die Risikominimierungsmaßnahmen benötigen gelb und Risiken die sehr kritisch sind rot.

Nach dem die Risiken bekannt sind werden entsprechende Maßnahmen gesetzt, um diese auf ein tragbares Maß zu bringen.

5 Technische und organisatorische Maßnahmen (TOMs):

Zunächst muss für jedes Risiko überlegt werden wie dieses bestmöglich beseitigt werden kann (organisatorische Maßnahme). Anschließend wird die Regelung/Maßnahme technisch umgesetzt (technische Maßnahme).

Um die Vertraulichkeit von Patienten zu gewährleisten wird für die Anwender und Administratoren ein Rollenmodell eingeführt. Dabei muss beachtet werden, dass Anwender und Admins unterschiedliche Berechtigungen haben und diese Berechtigungen nur durch eine Authentifizierung erhalten werden können. Die organisatorische Maßnahme ist, dass Anwender (Ärzte) nur auf Patientendaten zugreifen können, mit denen sie in einem Behandlungsverhältnis stehen und

die Admins überhaupt keinen Zugriff auf personenbezogene Daten haben dürfen (Datenschutz). Dies wird durch die technische Maßnahme so umgesetzt, dass es im System zwei Rollen gibt (Arzt, Admin), denen nach dem Login via zwei-Faktor-Authentifizierung mittels 1mal Tan und Username und Passwort, die entsprechenden Berechtigungen verteilt werden. Dies betrifft den Zugriffschutz auf relevante Daten. Um den Zutrittsschutz als weitete Risikominimierungsmaßnahme für den Verlust der Vertraulichkeit zu gewährleisten, sollen Ärzte nur Zutritt zu Räumen haben, die mit dem entsprechendem Patient dafür vorgesehen ist. Zudem soll Admins der Zutritt zu Behandlungsräumen komplett verweigert werden und nur im Stör- oder Notfall zugänglich sein (organisatorische Maßnahme). Um dies technisch zu realisieren verfügen Ärzte und Admins Chipkarten die unterschiedliche Berechtigungen haben. Um den Fall auszuschließen, dass ein Arzt Zutritt zu einem nicht vorgesehenen Raum hat, öffnet sich die Tür mit dem Chip nur, wenn im Datenbanksystem ein Eintrag vorliegt: z.B. Arzt Maier mit Patient Hans in Behandlungsraum 5. Die Chipkarten von den Admins gelten nur für die Serverräume und werden nur im Stör- oder Notfall automatisch umprogrammiert.

6 Qualitätsmanagement PDCA

PDCA-Zyklus: Für die Überprüfung der Maßnahmen, ob sie tatsächlich wirken, muss es einen regelmäßigen Kontrollprozess geben (Qualitätsmanagement). In der Planungsphase (P) werden die TOMs definiert und geplant. Im Do werden diese umgesetzt und implementiert. Im Check werden diese überwacht und die Planung mit den Ergebnisse verglichen. Im Act werden Fehler behoben und versucht den Prozess zu verbessern. Es ist wichtig für jedes Risiko die Maßnahmen regelmäßig zu überprüfen und auch immer wieder neue Bedrohungen in den Prozess miteinzubeziehen (z.B. Lessons Learned nach einem Notfall).

7 Vorgehensweise Ausfallssicherheitskonzept

Um die regulatorischen Anforderungen des NISG zu erfüllen muss ein Störfallprozess implementiert werden, der als weitere organisatorische Maßnahme betrachtet werden kann.

Es wird eine Stelle in der Praxis eingeführt, die Störfälle entgegennimmt und gemeinsam mit einem Störfallsystem die eingehende Störmeldungen miteinander vergleicht, um mögliche Probleme zu clustern. Mitarbeiter haben somit die Möglichkeit bei einem Verdacht auf eine Störung diese umgehend zu melden. Die Meldestelle eruiert anschließend aus der Prozessübersicht welcher Prozess betroffen ist und weiß aus der Priorisierung welches Schutzziel betroffen ist, sowie wie hoch das Risiko ist. Wenn die Störung bekannt ist wird sie nach den vordefinierten Maßnahmen abgearbeitet (Störplan). Der Störplan muss jeden Prozess beinhalten und ständig erweitert werden.

In diesem Plan stehen Anweisungen wie bereits bekannte Störungen zu beseitigen sind und wie die Organisation im Störfall agieren soll. Aus dem SLA ist bekannt wie wichtig das Service für den Kunden ist und welche Ausfallzeiten und Betriebszeiten berücksichtigt werden müssen. Goldene Prozesse sind kritisch und dürfen maximal 3 Stunden in den Betriebszeiten ausfallen. Silberne dürfen maximal 6 Stunden ausfallen und bronzefarbene Prozesse 12 Stunden. Kann eine Störung innerhalb der maximalen Ausfallzeit nicht behandelt werden (3 Stunden) so sind erstens Strafzahlungen zu bezahlen und zweites die Behörde zu informieren. Tritt dies ein handelt es sich um einen Notfall und der Notfallmanager (zugewiesene Rolle) ruft einen Notfall aus. Da es sich um eine dynamische Lage handelt läuft die Organisation im Notmodus und es gelten anderen Regelungen sowie ein eingeschränkter Betrieb. Bei einem Notfall wird das CERT umgehend informiert und in Zusammenarbeit versucht die Fehler zu beheben. Zudem wird der wesentliche Betrieb (Diagnostik, Therapie von Patienten) stark eingeschränkt und zusätzliche Informationssicherheitsexperten angefordert. Patientenbelege werden auch in Papier behalten und mögliche Verlorene Daten händisch gespeichert und nach Abschluss des Notfalls im System nacherfasst. Wenn bei einer Störung personenbezogene Daten im Spiel sind und diese innerhalb von 72 Stunden nicht behoben wird muss ebenfalls die Behörde informiert werden.