Protokoll:

Gesetzlich vorgegeben oder nicht es geht darum das Risiko zu vermindern. Dies geschieht durch gewisse Normen. Eine eigene Risikobeschreibung 31000 ISO. Wie geht man da ran? Insgesamt 9 Schritte

1. Schritt: Identifizierung wichtiger Prozesse und Assets (verschiedenste Güter z.B. Daten, Systeme).
   Medizinischer Bereich:
   - Input: kranker Patient
   - Output: gesunder Patient
2. Schritt: Prüfen auf bereits bestehenden Bedrohungskatalog. Wenn vorhanden dann darauf zurückgreifen. Bedrohungen werden im Kontext zu unseren Bedrohungen und Assets betrachtet. Hat ein gewisser Prozess eine Anfälligkeit auf Bedrohung? Wenn ja dann überlegen, wie dieser Prozess sichergestellt werden kann

3. Schritt: Schwachstelle

4. Schritt: Risikobewertung/ Risikoanalyse der Risiken welche zu Schwachstellen führen. Nach Kritikalität bewerten.
5. Schritt: Bestimmte Maßnahmen definieren, damit dieses Risiko minimiert wird. Verhindern geht nicht nur das Minimieren ist möglich.
6. Schritt: Implementierung von den Maßnahmen, damit die Prozesse und Assets sichergestellt werden können. PDAC-> Die Maßnahmen müssen überprüft werden, damit diese effektiv sind und wirken. KVP setzt auf jede einzelne Maßnahme.
7. Schritt: Überwachung der Maßnahmen. Immer Überprüfen ob die Maßnahme Stand der Technik entspricht und die Schritte am letzten Stand sind
8. Schritt: Gesamte Überwachung der Punkte 1-7. Da der Prozess oder die Werkzeuge sich im Laufe der Jahre verändern kann.
9. Schritt: Über das gesamte System drüber muss dokumentiert werden. Dient als regelmäßige Kontrolle und Nachweis.

All diese Punkte und der Ablauf sind der Risikoprozess, entweder ISO 27000 oder ISO 31000.

Es müssen Ausnahmen definiert werden -> Risikoanalyse.

Um Gefahren für den Patienten bei einer Behandlung zu minimieren, gibt es Policies. Update Policy _> Die Geräte dürfen nur außerhalb der Benutzungszeiten geupdated werden. Minimierung der Verwundbarkeit kann durch das Separieren der Netze erreicht werden. Kann soweit gehen dass kein Username oder Passwort auf den Systemen verwendet werden. Schützen vom Vorgang.

Wichtig bei den Maßnahmen. Die Maßnahmen bestehen aus organisatorischen und technischen Vorgaben, welche durch die DSGVO geschieht.