Sicherheitsempfehlung für transportable Datenträger im Universitätsklinikum-Essen

Grundsätzliches

- Das Speichern von Patientendaten auf lokalen, sowohl auf stationären, als auch auf mobilen EDV-Systemen und auf externen Speichermedien ist im Konzept nicht vorgesehen und macht der Nutzer auf eigenes Risiko und ist im Grunde nicht statthaft. Alle Patientendaten liegen zentral.
- Die Verantwortung von lokalen Daten und transportablen Datenträgern trägt der Nutzer.
- Alle EDV-Systeme sind über einen personifizierten Zugang mit Kennwort auf Betriebssystemebene zu schützen. Zugangsdaten dürfen nicht an Dritte weiter gegeben werden.

Um eine Datensicherheit für transportable Datenträger zu gewährleisten, empfiehlt die ZIT folgende Sicherheitseinstellung:

Notebooks:

Die von der ZIT als Standard definierten Notebooks (Lenovo ThinkPad) sind wie nachfolgend zu sichern:

- Schützen Sie das Notebook im BIOS mit System- und Festplattenkennwort.
- Falls das System verloren geht, ist es niemandem möglich das Notebook zu starten. Während des BIOS-Start wird nach Kennwort gefragt. Wenn die Festplatte entnommen und in einem anderen System montiert wird, wird der Anwender nach dem Passwort gefragt. Das bedeutet, dass die Hardware nutzlos ist und die Daten sicher bleiben.
- Verschlüsselt sind die Daten in diesem Fall aber nicht.

USB-Sticks:

Hier empfiehlt die ZIT einen USB-Stick mit einer hardwarebasierten 256-Bit AES-Verschlüsselung.

Entsorgung alter Speichermedien:

Elektronische, optische und magnetische Speichermedien, die Defekt sind oder nicht mehr benötigt werden, können bei der ZIT abgegeben werden. Bei der ZIT werden diese Speichermedien mechanisch zerstört und werden zur Entsorgung freigegeben.