

## Datenschutz am Universitätsklinikum Würzburg

Die klinikinternen Datenschutzbestimmungen, insbesondere die Datenschutzrichtlinie für das UKW, die Dienstanweisung IT-Arbeitsplätze sowie die Dienstanweisung Datenpannen sind einzuhalten.

Die genannten Regelungen sind im Intranet unter **Stabsstellen | Datenschutz | Datenschutzbestimmungen / Dienstanweisungen** zu finden.

Insbesondere zum Schutz des Rechts der Patientinnen und Patienten\* auf informationelle Selbstbestimmung sind die folgenden Punkte strikt einzuhalten:

- Schon die Tatsache, dass eine Person Patient des Klinikums ist, unterliegt der Schweigepflicht. Die Weitergabe sämtlicher Patientendaten an unberechtigte Dritte, auch in mündlicher Form, ist nicht zulässig und kann eine strafbare Verletzung der Schweigepflicht (§ 203 StGB) darstellen.
- Die Pflicht zur Verschwiegenheit in Hinblick auf Patientendaten besteht auch nach eventueller Beendigung der Tätigkeit am Klinikum fort.
- Bei telefonischen Auskunftersuchen muss sichergestellt werden, dass der Anfrager wirklich die berechtigte Stelle/ Person ist, erforderlichenfalls durch Rückruf. Aus Sicherheitsgründen sollte die Auskunft - soweit möglich - schriftlich per Post an die berechtigte Stelle/Person gegeben werden.
- Während Telefonaten ist sicherzustellen, dass die Vertraulichkeit gewahrt ist und keine unberechtigten Personen mithören können. Dies gilt insbesondere bei Verwendung von DECT- oder Mobiltelefonen.
- Telefax-Übermittlung von Patientendaten nach Extern ist nur im Ausnahmefall (z.B. akute Lebensgefahr oder wenn es die Dringlichkeit gebietet und der Patient in die Telefaxübermittlung nach Aufklärung über die Gefahren eingewilligt hat) zulässig.
- Auch intern ist die Telefax-Übermittlung von Patientendaten nur in Ausnahmefällen gestattet, d. h. wenn es die Dringlichkeit gebietet oder betriebsorganisatorische Abläufe dies unabdingbar machen, z.B. bei der Anforderung von Blutkomponenten über die Transfusionsmedizin und von Zytostatika über die Apotheke). Hierbei müssen aber besondere Sicherheitsvorkehrungen (z.B. Nutzen von Kurzwahlteilen) beachtet werden.
- PC-Monitore sind so auszurichten, dass eine unberechtigte Kenntnisnahme der Anzeige nicht möglich ist. Dies gilt auch für mobile Geräte wie Notebooks, Tablet-Rechner und Smartphones, insbesondere bei Verwendung außerhalb des UKW.
- PC-Arbeitsstationen sind bei Verlassen zu sperren („Windows-Taste“ und Buchstabe „L“) oder abzumelden („Start“ und dann „Abmelden“).
- Persönliche Passwörter sind vertraulich zu behandeln, die offene Aufbewahrung oder Weitergabe an andere Personen ist nicht zulässig. Es dürfen ausschließlich EDV-Benutzerkonten verwendet werden, für die eine offizielle Berechtigung besteht.
- Krankenakten, OP-Bücher und -Pläne, Patientenlisten, Behandlungsprotokolle (Operation, Anästhesie, Funktionsdiagnostik etc.) und sonstiges Material, das patientenbezogene Daten enthält oder mit personenbezogenen Patientendaten versehen ist (wie z.B. Infusionsbehältnisse und Patientenarmbänder, aber auch Gewebe-, Labor-, und mikrobiologische

\* Nachfolgend wird aus Gründen der besseren Lesbarkeit bei geschlechtsspezifischen Begriffen die maskuline Form verwendet. Diese Form versteht sich explizit als geschlechtsneutral. Gemeint sind selbstverständlich alle Personen gleich welchen Geschlechts.

Proben, etc.) müssen nach den strengsten Kriterien des Datenschutzes behandelt werden. Dies gilt auch für kopierte Patientenlisten, die z.B. bei klinischen Studien benutzt werden.

- Krankenakten und sonstige patientenbezogenen Unterlagen sind so aufzubewahren, dass die unberechtigte Kenntnisnahme ausgeschlossen ist. Das betrifft u.a. den Transport von Krankenakten auf Visitenwägen. Räume, in denen solche Unterlagen aufbewahrt werden (z.B. Stations- und Arztzimmer, Aufnahmebereiche Archive etc.), sind bei Verlassen durch die letzte Person abzuschließen.
- Mit Krankenakten und sonstigen patientenbezogenen Unterlagen, die nicht anonymisiert wurden, darf ausschließlich innerhalb der Klinik- bzw. Institutsräumlichkeiten gearbeitet werden. Diese Unterlagen dürfen niemals das Klinikumsgelände verlassen, um sie z.B. mit nach Hause zu nehmen. Dies gilt gleichermaßen für Fotokopien, Fotografien, Abschriften, Hardcopies etc. sowie für auf elektronischen Datenträgern (z.B. Laptops, USB-Sticks, Speicherkarten, etc.) gespeicherte Daten.
- Bei der Vernichtung von Krankenakten und sonstigen patientenbezogenen Unterlagen sind die gesetzlichen Aufbewahrungspflichten, die Dienstanweisung Abfallentsorgung sowie die Dienstanweisung Dokumentation und Archivierung von Krankenakten am UKW zu beachten.
- Die Vertraulichkeit personenbezogener Daten ist auch im Rahmen von Forschung und Lehre zu wahren. Sobald dies nach dem Forschungszweck möglich ist, sind Forschungsdaten zu anonymisieren. Studierende dürfen Daten nur in anonymisierter Form erheben und für wissenschaftliche Arbeiten (z.B. Dissertation) speichern.
- Die Nutzung des dienstlichen E-Mail-Accounts zu privaten Zwecken ist nicht zulässig. Dies gilt grundsätzlich auch für den dienstlichen Internetanschluss; Ausnahmen dazu regelt § 9 der Dienstanweisung IT-Arbeitsplätze.
- Der Versand personenbezogener Daten per E-Mail innerhalb der IT-Infrastruktur des UKW (Versand an eine E-Mail-Adresse mit der Endung ...@ukw.de) ist ohne Inhaltsverschlüsselung zulässig. Unverschlüsselte E-Mails, die die IT-Infrastruktur des UKW verlassen, dürfen keine besonders schutzwürdigen personenbezogenen Daten enthalten. Besonders schutzwürdig sind Daten, die Bestandteil der Personalakte sind sowie alle personenbezogenen Patientendaten mit Ausnahme rein organisatorischer Inhalte wie z.B. Terminbestätigungen oder -erinnerungen. Bei E-Mails mit solchem Inhalt ist darauf zu achten, dass keine Rückschlüsse möglich sind, welche gesundheitlichen Beeinträchtigungen der Empfänger hat.
- Die automatische Weiterleitung von internen E-Mails an eine E-Mail-Adresse außerhalb der IT-Infrastruktur des UKW ist untersagt.
- Die Übermittlung von besonders schutzwürdigen personenbezogenen Daten per WhatsApp oder ähnlichen Messangern ist nicht zulässig.
- Die Dienstanweisung Datenpannen verpflichtet alle Beschäftigten, Datenschutzverletzungen unverzüglich per E-Mail an [datenpanne@ukw.de](mailto:datenpanne@ukw.de), alternativ telefonisch an die Hotline des SMI (Tel.: 201-55473), zu melden.

In Zweifelsfällen stehen die internen Datenschutzbeauftragten sowie der behördliche Datenschutzbeauftragte des Klinikums zur Verfügung.

Gelesen und zur Kenntnis genommen, ein Exemplar dieser Hinweise ist mir ausgehändigt worden.

---

Ort, Datum

Unterschrift