

P r e s s e release

December 13, 2018

711.395.2

Examination of an electronic health record by the

Berlin Commissioner for Data Protection and Freedom of Information

The Berlin Commissioner for Data Protection and Freedom of Information is currently examining one

Electronic health records funded by health insurance companies and private health insurance companies

on compliance with data protection and data security regulations. The product

enables patients to access documents and data about their health and

collect medical treatment. Providers of medical services can

ask Patient data to be included in the electronic health record. Also health insurance companies

and insurance companies can use the file to specifically address their insured,

subject to their consent.

As part of this audit, various deficiencies in relation to the information of the

insured persons, obtaining consent, ensuring data security and

the implementation of a data protection impact assessment. The provider now receives

Opportunity to comment on the identified deficiencies and to rectify them. In pieces

this has already happened.

In this context, the Berlin Commissioner for Data Protection and Freedom of Information

hang already doctors who are asked to enter data in the health record

set to the following:

Medical service providers are not obliged to store patient-related data in a

enter electronic health records. Although Art. 15 Para. 3 Sentence 2 data protection

Basic Regulation data subjects have the right to an electronic copy of them

Responsible: Joachim-Martin Mehlitz

Office: Cristina Vecchi

Email: presse@datenschutz-berlin.de

Friedrichstr. 219

10969 Berlin

Tel: 030 13889 - 0

Fax: 030 2155050

- 2 -

obtain relevant data. However, the service providers can use the route to the transmission

You can choose the electronic copy yourself, as long as this makes it easier for the person concerned to receive it
person is not made more difficult.

Medical service providers may only transfer patient-related data to operators

transmit electronic health records if the corresponding request is actually

emanating from the person being treated. The service providers must take care of this themselves

and convince them on their own responsibility, whereby in particular the authenticity of the silent

declarations of compulsory release must be checked. A transmission without one

Permission is not only a breach of privacy, but also a violation of the

medical confidentiality.

Any transmission of patient-related data must comply with data security requirements

suffice. Not only the diagnosis and the type of treatment require a special

Confidentiality, but already the fact that any treatment at all by a

specific service provider has taken place. Data security must be carried out both by

Operators of the electronic health record are guaranteed, as well as from the medical
cal service providers.

Patient-related data should be encrypted by the service provider before transmission

rare that only the treated person can carry out the decryption himself.

In this case, the service provider must ensure that the encryption only

is done with the key provided by the person being treated, and must

In case of doubt, be able to prove that the correct key was used.

Unencrypted patient-related data should not be processed on workstation computers

who can access the Internet unhindered. This corresponds to the recommendations

the National Association of Statutory Health Insurance Physicians and the German Medical Association.

Maja Smolczyk:

“Electronic health records offer patients the opportunity to

Store and manage health data in a central location. The potential benefits

that may result from this, however, must not be at the expense of data protection and

data security go. The data protection requirements must therefore already be met

should be taken into account and implemented when designing the corresponding offers.”