Talkey

Communicate securely with your clients

Solution demand in health care

Security of e-mail communication

Data leakage prevention

GDPR **Protection** of personal data

Reputation protection

What and with whom you communicate

Internal communication

employees, management
inputs and outputs from/to
applications and systems
personnel department

Who?
With whom?

External communication

patients and clients
external lawyers, advisers
government administrations
business partners
e-mail room

negotiation documents, personal data,
financial results, payslips,
labour law documentation,
tender documents for tenders

What?
What sort of content?

e-prescriptions
health reports
health competence reviews
examination requests
patients and clients personal data

What solution you look for

Simple encryption of e-mails,
files and folders on PC

Possibility of limitation of
sending personal data in an
insecure way

Digital signature - confirmation
of sender identity

Fast implementation and
inexpensive infrastructure

Access denial to messages in case
of an employee leaving or
business partner changing

Full user control over
the system running

Time limitation of access
to messages

Free of charge content
decryption by an external
recipient without the need of
installation or registration

Assurance of message not
being read by anyone other
than the sender and the
recipient

If you send anything by an e-mail, you would not write onto a postcard, encrypt it.

Your e-mail, as well as a postcard can be read by whoever going by.

Good day Mr. Pill,

Please see the attached
your examination request.
Please make your appointment till
the end of this week.

Best regards,
your medic

Dan Pill
Postal Street 123/4
Ostrava

7 0 2 0 0

Czech Republic

3 reasons why encryption with Talkey is the most safest way of e-mail communication

1 Guarantee your identity

Encrypted message by Talkey guarantees the origin, the authorship and the stability of a message. Your clients and partners know that they should open only encrypted e-mails received from you, which protect them from cheated message, which will misuse your company domain. You, on the other hand, know that you are taking every step possible for protecting your client's data and therefore preventing court cases, financial losses and the loss of reputation.

2 Be in control over the way how the recipient will treat your message

Set what the recipient can or cannot do with your message. Protect information and data sent by e-mails. For instance, you can prohibit the recipient from forwarding your message, determine how many times or how long for the message can be opened, until it is invalid and therefore impossible to decrypt.

these advanced features will help you with that

3 Take really back a wrongly sent e-mail

Do you know that, in reality, a common e-mail client can not delete an e-mail, even though you click on "take back" button? Such e-mail will stay hanging in between the servers and could be read by anybody, basically. Talkey enables to make a sent e-mail invalid, which means, that the e-mail could not be opened neither by the recipient or anyone else.

disable the recipient's ability to forwarding your message

set the number of times the message can be opened

limit the amount of time your message to be visible

do not allow the message to be displayed on mobile device