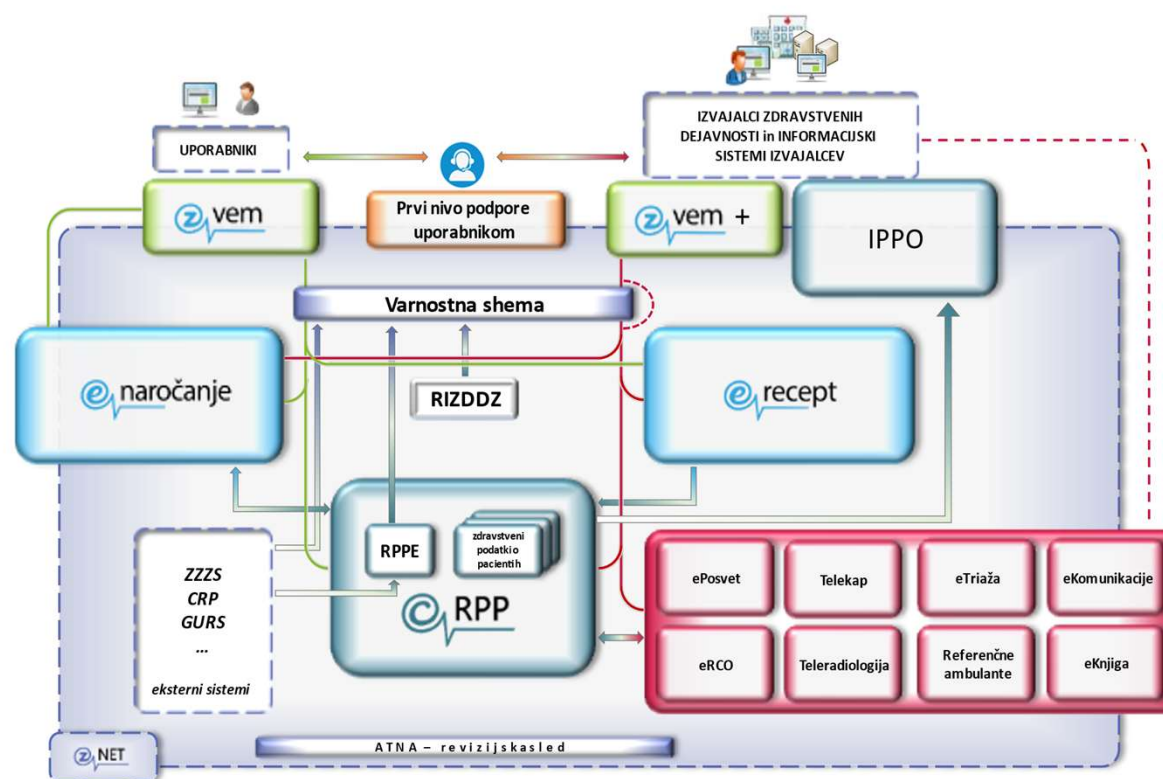


Predstavitev vodenja področja informacijske varnosti za rešitve eZdravja

dr. Matjaž Drev,
Nacionalni inštitut za javno zdravje

eZdravje: vsi podatki na enem mestu



(Ne)varen ekosistem

Javni zdravstveni zavodi:

- 2 univerzitetna klinična centra
- 10 splošnih bolnišnic
- 16 specialističnih bolnišnic
- 64 zdravstvenih domov
- 24 javnih lekarn
- 5 drugih (ZTM, NIJZ, NLZOH, Slovenija Transplant, MKZ Rakitna)

Zasebniki s koncesijo

- (približno) 1400

(vir: Pregled stanja na področju zdravstva v Sloveniji - januar 2023; Letno poročilo Zavoda za zdravstveno zavarovanje Slovenije za leto 2023)

Vse za zdravje pacientov?

- **Viri so omejeni** in usmerjeni v obravnavo pacientov.
- Časi se spreminjajo: informatizacija bolnišničnih sistemov prinaša vrsto varnostnih tveganj: **zdravstveni podatki so digitalizirani, medicinske naprave vse bolj “pametne”**.
- (Ne)zrelost obravnavanja informacijske varnosti je med posameznimi IZD **zelo heterogena**.
- **Sistematičen pristop** k upravljanju informacijske varnosti **ni pravilo**: pogosto se zatakne že pri pregledu IT opreme in izvedbi analize tveganj.
- **Kljub temu: večina IZD ima vzpostavljene osnovne** organizacijske in tehnične **vidike varovanja podatkov; posamezni IZD to področje urejajo zelo dobro**.

Kaj se (ne) dogaja?

- **MZ + NIJZ + (javni) IZD + ZDRZZ (2018 – 2021):** določitev osnovnih varnostnih zahtev in priprava vzorčne dokumentacije s področja informacijske varnosti; več pozivov k sprejemanju teh zahtev; več delovnih sestankov; delni uspeh.
- **URSIV, SI-GOV CERT, SI-CERT, MORS, ENISA, NATO** skupaj z drugimi deležniki občasno organizirajo operativne vaje in varnostno preverjanje IT storitev.
- **MZ (2025 - ?):** oblikovanje skupine za informacijsko varnost.
- **DigiZdravje in ZDigZ (2026 ?)**
- **NIS 2 in ZInfV-1:** javni IZD so (večinoma) dobili status izvajalcev pomembnih storitev, zato so dolžni izpolnjevati obsežne zakonske zahteve glede informacijske varnosti, sicer tvegajo visoke globe.

Varovanje podatkov v eZdravju?

Ključne rešitve eZdravja (CRPP, zNET) so prepoznane kot **bistvene storitve (ZInfV-1)** in kot del **kritične infrastrukture (ZKI)**, zato morajo izpolnjevati obsežne zahteve obeh zakonov.

Infrastrukturni poudarki:

- Dostop do rešitev eZdravja večinoma znotraj VPN zNET (šifriran prenos podatkov).
- Popolna redundanca storitev in podatkov s pomočjo dveh geografsko ločenih podatkovnih centrov (na območju RS).
- Redno izvajanje varnostnih preverjanj ključnih rešitev.
- 24/7 varnostno operativni center.

Toda **uporabniki** (IZD, posamezni izvajalci) **morajo še vedno** (po)skrbeti za informacijsko varnosti na svoji strani!



REPUBLIKA SLOVENIJA
MINISTRSTVO ZA ZDRAVJE



NAČRT ZA
OKREVANJE
IN ODPORNOST



Financira
Evropska unija
NextGenerationEU

Hvala za pozornost.