Beveiligen van patiëntgegevens: Why Should I?

Edward Snowden heeft privacy weer op de kaart gezet. James Bond-liefhebbers halen hun hart op. Intussen vraagt u zich misschien af waarom u uw e-mailberichten met patiëntgegevens nog zou beveiligen. De NSA leest immers toch met u mee?

Privacy staat weer eens in het middelpunt van de belangstelling, mede dankzij Edward Snowden, voormalig CIA-medewerker die informatie lekte over de afluister- en spionageactiviteiten op internet door de Amerikaanse National Security Agency (NSA). De NRC-website biedt een indrukwekkend overzicht van onthullingen over de afluisterpraktijken van de Amerikaanse inlichtingendienst, zoals het aftappen van de mobiele telefoon van Angela Merkel, camerabeelden van ambassades en creditcardtransacties, maar ook de inhoud van beveiligde medische berichten.[1]

Het is een lijst waar liefhebbers van James Bond-films hun vingers bij aflikken. Maar ook een lijst om van te schrikken. Logisch dat burgers na het horen van de zoveelste NSA-onthulling denken: 'Zie je wel, er bestaat geen privacy meer'. En als arts vraagt u zich misschien af wat het nut nog is van het beveiligen van patiëntgegevens die u bijvoorbeeld per e-mail wilt versturen naar een collega. Waarom zou u, als de NSA zelfs beveiligde medische gegevens blijkt af te tappen?

U bent niet interessant genoeg voor de NSA

Allereerst lijkt het erop dat de NSA en de Britse inlichtingendienst vooral geïnteresseerd zijn in economische en politieke informatie en informatie om terroristische aanslagen te voorkomen. Wat u met collega's uitwisselt is voor de NSA niet zo interessant, tenzij u natuurlijk terroristen of captains of industry in uw praktijk hebt. Maar dan bent u waarschijnlijk al lang afgetapt door onze eigen inlichtingendienst, die per dag net zoveel smartphones aftapt als de VS in een heel jaar![2]

Bescherm uw vertrouwensrelatie met de patiënt

Maar afgezien van inlichtingendiensten moeten patiëntgegevens vooral beschermd worden tegen onbevoegde anderen. U heeft een vertrouwensrelatie met patiënten en dient in te staan voor de vertrouwelijkheid van hun gegevens. Dat is ook in uw belang trouwens, want u wilt vast niet dat uw praktijk negatief in de lokale media wordt genoemd omdat patiëntgegevens bij u niet in veilige handen zouden zijn.

Wettelijke verplichting tot beveiliging

Een derde goede reden om u druk te maken, vormt de Wet bescherming persoonsgegevens: hierin staat dat wie verantwoordelijk is voor het verstrekken van persoonsgegevens passende maatregelen moet treffen om deze te beveiligen. De nationale privacywaakhond, College bescherming persoonsgegevens (CBP) heeft voor najaar 2013 een nieuw onderzoek aangekondigd naar de beveiliging van het online aanvragen van herhaalrecepten. De LHV riep in oktober huisartsen dan ook op de beveiliging van hun web-sites nog eens goed te controleren, nu eerder een kwart van de huisartspraktijken een onbeveiligde verbinding bleek te gebruiken.[3]

Boete tot 1 miljoen euro

Houdt u zich niet aan de wet, dan loopt u de kans op een boete, die het CBP kan verbinden aan een dwangsom voor elke dag dat u de wet overtreedt. Een vierde reden dus voor een check van uw praktijk. De hoogte van de boetes verandert over een jaar of twee met de nieuwe Europese privacywetgeving. Dan kan dit oplopen tot één miljoen euro of 2 procent van uw jaaromzet.

Richtlijn omgaan met medische gegevens

Last but not least vereisen de KNMG Richtlijnen inzake het omgaan met medische gegevens dat u bij het online uitwisselen van patiëntgegevens gegevens minimaal versleuteld verstuurt. Zonder beveiliging loopt u het risico op een tuchtmaatregel of civiele aansprakelijkheid.

Vijf goede redenen dus om uitsluitend beveiligde patiëntengegevens elektronisch uit te wisselen. Why? That's why! *knmg*

Sjaak Nouwt
beleidsadviseur gezondheidsrecht KNMG

Meer informatie hierover en de voetnoten vind u op knmg.nl