Informatieveiligheid begint bij jou!

Vertrouwelijk omgaan met medische gegevens is in een ziekenhuis erg van belang. Mede door het open karakter van een ziekenhuis zijn de risico's groot. Enerzijds bestaan risico's van diefstal van waardevolle bedrijfsmiddelen, zoals bijvoorbeeld apparatuur, bezittingen van patiënten, maar ook medicijnen of andere middelen. Anderzijds bestaan ook risico's rondom (patiënt)informatie. Natuurlijk zijn er nog meer andere bedreigingen die risico's opleveren voor personeel en patiënten en ook die vragen om beveiligingsmaatregelen.

Zo was recent een item in het NOS-journaal over internetcriminaliteit. Op allerlei manieren wordt geprobeerd om illegaal toegang te krijgen tot computersystemen van grote organisaties. Ransomware, software dus die je computer of je computersysteem als het ware gijzelt, is en blijft een gevaar in de huidige digitale wereld. Een 'honderd procent bescherming' bestaat helaas niet, omdat criminelen wereldwijd hun pogingen steeds meer verfijnen. Wat dat betreft is het de uitdaging om, als Elkerliek en samenwerkende ziekenhuizen, die criminelen steeds een stapje voor te zijn.

Het Elkerliek doet er alles aan om zowel de patiëntveiligheid als de privacy van onze patiënten maximaal te waarborgen. Onze digitale verdedigingslinies staan elke dag paraat. Die paraatheid is er op drie niveaus. De eerste twee niveaus hebben te maken met preventie en detectie. We zorgen dus voor de meest actuele beveiligingssoftware, scannen inkomende berichten op mogelijke bedreigingen, blokkeren 'gevaarlijke' sites, maken actuele back-ups, we trainen medewerkers, geven voorlichting en adviseren. En gaat het tóch fout? Dan zorgen we er op het derde niveau voor dat de impact zo beperkt mogelijk blijft. Door snel en adequaat te reageren en volgens vaste procedures de aanval een halt toe te roepen, zorgen we dat schade beperkt blijft en onze dagelijkse zorg aan patiënten ongehinderd doorgang kan vinden. Kortom, dagelijks werken we met volle kracht om veiligheid en privacy optimaal te waarborgen.

En hoe goed is jouw informatiebeveiliging? In ons ziekenhuis werken we met erg veel persoonsgegevens. Dit zijn persoonlijke gegevens zoals: naam, adres, geboortedatum, telefoonnummer en huisarts. Daarnaast werken we met 'bijzondere' persoonsgegevens zoals: BSN en gezondheidsgegevens. We hebben persoonsgegevens van onze patiënten, maar vaak ook van de werknemers van het ziekenhuis. Deze gegevens moeten we goed beveiligen voor mensen die hier niets mee te maken hebben of zelfs kwaadaardige bedoelingen mee hebben. Ook wij als werknemers van het ziekenhuis hebben alleen recht op inzage wanneer we in het kader van onze functie die informatie nodig hebben.

Hier volgt een aantal spelregels rondom informatie beveiliging:

Kijk zelf niet in persoonsgegevens wanneer dat niet echt nodig is voor de uitoefening van je functie en taak op dat moment. Je mag dus ook niet in dossiers kijken van familie, vrienden en bekenden wanneer je niet betrokken bent bij de behandeling. Als je wel betrokken bent bij een behandeling mag je alleen in die informatie die jij nodig hebt voor jouw functie.

Berg je spullen op wanneer je de werkplek verlaat, of vraag iemand een oogje in het zeil te houden. Kasten met informatie sluit je af en de sleutel bewaar je op een veilige plaats.

Log je computer uit als je de werkplek verlaat. Geef niemand je wachtwoord en schrijf deze ook niet op een papiertje (post-it) wat op een vrij toegankelijke plaats ligt.

Wees alert met het achterlaten van je privé én werkgegevens op (onbetrouwbare) internetsites. Dit voorkomt onnodig SPAM en HOAX e-mail, danwel vroeg of laat wordt een website gehackt waarop je staat ingeschreven en ontstaat op die manier toegang tot jouw persoonlijke geregistreerde gegevens met alle gevolgen van dien.

Zorg dat niemand over je schouder mee kan kijken als je met belangrijke informatie bezig bent (patiëntengegevens). Wanneer je privacy gevoelige informatie bespreekt, zorg dat anderen niet mee kunnen luisteren.

Wanneer je persoonsgegevens moet uitwisselen doe dat dan veilig. Geen persoonsgegevens via de mail. Stuur gegevens ook alleen op als je zeker weet dat die persoon daar toegang tot mag hebben. Telefonisch verkregen adressen of faxnummers van te voren checken of ze kloppen. Weet je zeker dat de persoon aan de telefoon echt degene is die hij zegt te zijn. Met andere woorden, pas op voor “social engineering” waarbij iemand je misleidt waardoor je informatie geeft.

Printen is ouderwets. Doe dat dus zo weinig mogelijk. Als je toch persoonsgegevens moet printen, doe dat dan met follow me printen of haal je print meteen van de printer. Laat prints ook niet achter in vergaderruimtes of openbare ruimten.

Gebruik geen mail naar externen, dropbox en weTransfer voor het verzenden van patiëntgegevens. Deze zijn onvoldoende beveiligd.

De verzamelnaam voor kwaadaardige software is malware. Daaronder vallen ransomware, virussen, wormen, phising mails, trojan horses en spyware.

Meldt iedere malware of een vermoeden daarvan bij de service desk (5900) én je leidinggevende. Open geen verdachte mails, websites of applicaties maar verwijder ze meteen. Zo houd je jezelf, het ziekenhuis en je privé gezond!

Meer weten? Elkerliek traint haar mensen standaard op het borgen van informatieveiligheid. Vraag ernaar bij je leidinggevende!