Capio

Vi skyddar din information

Vårt informationssäkerhetsarbete och skydd av personuppgifter

Vår informationssäkerhetsstrategi

Capios förmåga att erbjuda sjukvård av högsta kvalitet stöds av vår strategi för informationssäkerhet och skydd av personuppgifter. Vid lagring och överföring av information måste vi säkerställa en ändamålsenlig säkerhet. Vi ser det som vår plikt att följa lagar och regler som styr insamling och behandling av personuppgifter. För oss är skyddandet av våra patienters rättigheter och integritet en förutsättning för att skapa förtroende gentemot våra patienter.

Vi skyddar våra, liksom våra patienters, informationstillgångar från obehörig insamling, bevarande, användning, utlämning, ändring och förstörelse. Detta åstadkoms genom ändamålsenliga policys, riktlinjer, rutiner och teknisk säkerhet. Våra medarbetare är förpliktigade att följa våra styrande dokument, liksom lagar och regler.

Capios informationssäkerhetsansvariga och dataskyddsombud arbetar under koncernens policy och riktlinjer, som ska följas inom samtliga affärsområden. Detta bidrar till en enhetlig säkerhet av våra informationstillgångar och de personuppgifter vi behandlar.

Personuppgiftspolicy

Capios personuppgiftspolicy innehåller principer för behandling av personuppgifter, vilket ger ett ramverk för behandling av personuppgifter i enlighet med dataskyddslagar och internationella standarder. Vår personuppgifts-policy utgår från följande principer:

- Vid behandling av personuppgifter, skyddar vi registrerades rättigheter. Personuppgifter samlas in och behandlas lagligt och rättvist.
- Personuppgifter behandlas för uttryckliga och legitima syften.
- Den registrerade är informerad om hur hans/hennes personuppgifter behandlas.
- Personuppgifter måste vara relevanta och inte överflödiga i relation till personuppgiftsbehandlingens syfte.
- Personuppgifter raderas då de inte längre behövs, efter hänsyn till legala krav på lagringstider.
- Ändamålsenliga åtgärder vidtas för att säkerställa korrektheten av personuppgifter.
- Personuppgifter hanteras som konfidentiella och säkert med ändamålsenliga organisatoriska- och tekniska säkerhetsåtgärder.

Informationssäkerhetspolicy

Capios informationssäkerhetspolicy innehåller informationssäkerhetsstandarder och anger övergripande säkerhetskrav inom organisationen. Detaljerade krav finns beskrivna i informationssäkerhetsriktlinjerna.

Informationssäkerhetskrav berör vedertagna informationssäkerhetsområden, inkluderande men inte begränsat till:

- Övervakning och efterlevnad
- Åtkomstsäkerhet
- Driftsäkerhet
- Kommunikations- och nätverkssäkerhet
- Fysisk säkerhet
- Personalsäkerhet
- Kontinuitetsplanering
- Riskhantering
- Informationsklassificering

Medvetenhet och utbildning

Information, vägledning och utbildning vi erbjuder vår personal hålls kontinuerligt uppdaterade, då hot och risker ständigt förändras. Att skapa medvetenhet om hot och risker påverkande informationssäkerhet och personuppgiftsbehandling är en ständigt pågående process. Det är en process som vi arbetar aktivt med, vilket reflekteras inte endast i utbildningsinsatser utan i flera andra aktiviteter för att driva medvetenheten inom organisationen.

Säkerhetsstrategi och synsätt

Capios informationssäkerhetsarbete är förankrat genom vår informationssäkerhetspolicy. Arbetet är utformat för att driva och främja konfidentialitet, integritet och tillgänglighet för våra informationstillgångar, och personuppgiftsbehandlingar. Vi stödjer arbetet genom säkerhetsåtgärder i enlighet med lagar och regler, och i enlighet med internationella standarder.

Capio arbetar i informationssäkerhetsarbete proaktivt med att säkerställa och hantera konfidentialitet avseende personuppgifter, vilket inkluderar:

- Ändamålsenliga policys och riktlinjer
- IT-säkerhetsåtgärder
- Revision och uppföljning
- Incidenthantering för effektiv hantering och åtgärd av säkerhetsrelaterade incidenter

Teknisk säkerhet

Capios arbete med informationssäkerhet är mer än beslutade policy och riktlinjer. Vi säkerställer konfidentialitet, integritet och tillgänglighet av information genom skydd av våra tekniska resurser och informationstillgångar. Säkerhetsåtgärder inkluderar, men är inte begränsade till:

- Brandvägg
- Skydd mot skadlig kod
- Lösningar för flerfaktorsautentisering
- Säkerhetsuppdateringar och bedömning av sårbarheter
- Fysiska kontroller, så som tillträdeskontroller
- Lösningar för förhindrande av, och upptäckt av intrångsförsök
- Övervakningssystem

Revision och uppföljning

Vi genomför revision och uppföljning för att följa upp efterlevnaden av policy och riktlinjer. Vi hanterar följsamhet avseende krav på personuppgiftsbehandling och informationssäkerhet genom att kontinuerligt genomföra följande revisioner och uppföljningar:

Konsekvensanalyser

Capio genomför konsekvensanalyser avseende personuppgiftsbehandlingar. Varje konsekvensanalys bedömer berörda applikationer mot våra informationssäkerhetsstandarder, och innehåller vid behov rekommendationer för att hantera risker för den personliga integriteten.

Utvärderingar av kontrollers effektivitet

För att verifiera att kontroller är implementerade och fungerar korrekt över tiden, genomför Capio olika uppföljningar och bedömningar av kontrollers effektivitet, inkluderande:

- Sårbarhetsanalyser för nätverk och applikationer, vilka fokuserar på den tekniska säkerheten, så som säkerhetsuppdateringar, applikationssäkerhet och infrastruktursäkerhet.
- Bedömning av kontrollers effektivitet, vilket inkluderar granskning av både tekniska kontroller och rutiner.
- Löpande övervakning av kontrollers effektivitet, för att säkerställa att kontroller är korrekt uppsatta.

Informationssäkerhetsrevision

Våra applikationer, tjänster och datacenters revideras:

- Revisionsinsatser inkluderar intervju med nyckelpersonal, genomgångar av rutiner och granskningar för att bedöma efterlevnaden av policy och riktlinjer, liksom lagar och regler.

Självutvärderingar

För att etablera en fullständig översikt av vår informationssäkerhetsefterlevnad, genomför vi årliga självutvärderingar för att utvärdera efterlevnaden mot våra policys och riktlinjer.

Informationssäkerhetsbrister sammanställs och bedöms av ledningen. Vid behov definieras och beslutas åtgärdsplaner.

Sammanfattning

Capio säkerställer informationen för våra patienter och intressenter genom vår informationssäkerhetsstrategi, och strategi för personuppgiftsbehandling:

- Vi har en enhetlig styrning av informationssäkerhet och personuppgiftsbehandling för att säkerställa ett ändamålsenligt skydd av våra informationstillgångar och personuppgifter vi behandlar.
- Vi genomför både konsekvensanalyser, avseende personuppgiftsbehandlingar, och säkerhetsuppföljningar/revision av våra applikationer – både i samband med införande och i produktion.
- Vi skyddar personuppgifter genom ändamålsenliga fysiska, tekniska och organisatoriska säkerhetsåtgärder.
- Våra avtal med tredjeparter, som hanterar information på uppdrag av oss, innehåller krav på säkerhetsåtgärder i enlighet med våra policys, riktlinjer och kontroller för att säkerställa att informationen hanteras säkert och korrekt.

Intressenter och individer kräver ansvar från de organisationer som hanterar deras personuppgifter och konfidentiella information. Vi förstår vikten av att vidta lämpliga åtgärder för att skydda informationen och arbetar aktivt för att skydda information om våra patienter, våra medarbetare och våra intressenter.

Vänligen kontakta oss på Capio om du har några frågor eller vill ha ytterligare information om hur vi skyddar din information.