Implementering af iPad til patienter

Indstillingsvejledning

Indhold

Oversigt

Sundhedssektoren fokuserer i stigende grad på at inddrage patienterne og give dem en god oplevelse gennem hele behandlingsprocessen. Implementering af iPad med apps, der har patienten i centrum, gør det muligt for hospitaler at forbedre hvert trin i patientens forløb, fra indlæggelse til udskrivelse. Med iOS-apps fra tredjepartsudviklere kan hospitaler give patienter mulighed for at se deres daglige tidsplan, komme i kontakt med plejeteamet, holde øje med deres fremskridt, blive klogere på behandlingsplanen og finde underholdning efter egen smag – så patienten er i centrum.

Denne vejledning er en hjælp til hospitalets IT-medarbejdere, når de skal konfigurere og implementere iPad til patientbrug. iPad kan prækonfigureres med minimal indstilling, så patienter får adgang til iOS-apps, og IT-afdelingen kan beskytte patientdata vha. administration af mobile enheder (MDM) og samtidig skabe en fantastisk brugeroplevelse. Når en patient er udskrevet, kan iPad på sikker vis slette alle patientdata og nulstilles til fabriksindstillingerne, så den er klar til at blive brugt af næste patient.

Ved implementering af iPad til patienter er det vigtigt at beslutte, om I vil opbevare enhederne på stuen eller centralt (se afsnittene Opbevaring på stuen og Central opbevaring). Opbevaring på stuen er muligt, da iPad-enheden kan nulstilles, og data slettes trådløst. Enhederne kan derfor blive på stuen hele tiden. Mange hospitaler foretrækker denne løsning, fordi den minimerer sygeplejerskernes og andet personales arbejde. Samtidig kan der være tungtvejende grunde til at implementere central opbevaring, f.eks. hvis der er færre iPad-enheder end stuer, eller hvis der er personale til rådighed eller frivillige, som kan holde styr på enhederne, når patienterne bliver indlagt eller udskrevet.

Uanset hvilket implementeringsscenarie I vælger, er alle de forberedende trin i denne vejledning vigtige for at opnå en vellykket implementering.

Forberedelse

Dette afsnit beskriver fire trin, der skal følges under forberedelsen til implementering af enheder og apps på hospitalet.

Evaluering af infrastrukturen

Første trin er at evaluere jeres netværksinfrastruktur. Hospitalets fysiske rammer og folks adfærd inden for disse områder er af afgørende betydning for, hvordan I planlægger jeres netværk, Wi-Fi-dækning og kapacitet.

Wi-Fi og netværk

Det er vigtigt med konsistent og pålidelig adgang til et trådløst netværk til indstilling og konfigurering af iOS-enheder. Undersøg, om jeres hospitals Wi-Fi-netværk understøtter forbindelse til flere enheder på samme tid fra alle jeres brugere. I skal muligvis også konfigurere jeres webproxy- eller firewall-porte, hvis enhederne ikke kan få adgang til Apples aktiveringsservere eller iTunes Store. Apple og Cisco optimerer netværksoplevelsen for enheder med iOS 10 eller nyere. Kontakt jeres repræsentant fra Apple eller Cisco for at få de nyeste oplysninger om disse netværksfunktioner.

Caching af indhold

I macOS sørger en integreret funktion – indlæsning af indhold i buffer – for at lagre en lokal kopi af ofte anvendt indhold fra Apple-servere, så systemet kræver mindre båndbredde, når det overfører indhold på netværket. Med caching af indhold går det hurtigere at hente og levere software via App Store, Mac App Store, iTunes Store og iBooks Store. Den kan også gemme software-opdateringer i cachen, så de hurtigere kan overføres til flere iOS-enheder. Caching – eller indlæsning af indhold i buffer – omfatter tjenesten tethered caching, som gør en Mac i stand til at dele sin internetforbindelse med et stort antal iOS-enheder tilsluttet via USB.

Invester i en MDM-løsning

Med MDM kan hospitaler registrere iOS-enheder i deres miljø på en sikker måde, konfigurere og opdatere indstillinger trådløst, oprette regler, implementere og administrere apps samt slette eller låse administrerede enheder eksternt. Disse funktioner er en del af iOS og aktiveres af MDM-løsninger fra tredjeparter. Der findes MDM-løsninger fra en lang række leverandører, og de kan enten være cloud-baserede eller installeres internt. MDM-løsningerne fås med forskellige funktioner og i forskellige prisklasser, så I selv kan vælge den løsning, der passer bedst til jeres behov. Nogle leverandører af MDM-løsninger tilbyder også indstillinger, der er defineret i forvejen, så det bliver nemmere at konfigurere enheder til patientbrug.

Oprettelse af en konfiguration

Når I har valgt en MDM-løsning, skal I oprette en konfiguration, der er optimeret specifikt til jeres patienters brug og kan installeres trådløst via jeres MDM-løsning. En konfiguration har normalt indstillinger og begrænsninger, der definerer enheden på en måde, der gør den velegnet til patientbrug. Disse indstillinger vil være med til at gøre patientens første oplevelse mindre kompliceret og kan samtidig deaktivere funktioner og tjenester, der gemmer personlige data eller blot er unødvendige.

Begrænsninger

Følgende er eksempler på begrænsninger, som I bør overveje at deaktivere, så der ikke gemmes personlige oplysninger på enheden. **Bemærk:** Beskrivelserne kan variere afhængigt af den konkrete MDM-løsning.

Administration af enheder: Tillad ikke manuel installation af profiler, tillad ikke konfiguration af begrænsninger, tillad ikke ændring af enhedens navn, tillad ikke kontoændringer, påtving begrænset reklamesporing, og tillad ikke pardannelse med værter, som ikke findes i Configurator.

Administration af data: Tillad ikke dokumenter fra administrerede kilder i ikke-administrerede destinationer, tillad ikke ikke-administrerede dokumenter i administrerede destinationer, og påtving AirDrop status som en ikke-administreret destination.

Apps: Tillad ikke App Store-symbolet på hjemmeskærmen, tillad ikke fjernelse af apps, tillad ikke køb i apps, tillad ikke brugeren at godkende ikke-administrerede virksomhedsapps, og skjul bestemte apps på hjemmeskærmen.

Medier: Tillad ikke brug af iTunes Store, tillad ikke brug af iBooks Store, tillad ikke Game Center, fjern markeringen af påtving indtastning af adgangskode til iTunes Store, og begræns medieindhold efter behov.

Hjemmeskærmens layout, funktionen Mistet og andre indstillinger

I kan styre, hvordan apps, mapper og webklip er arrangeret på hjemmeskærmen på de overvågede enheder. Slå brug af kamera til, så hospitalets personale kan scanne en patients QR-kode med en sikret patient-app eller føje et billede af patienten til en elektronisk patientjournal-app (EPJ). For at kunne spore mistede iPad-enheder skal I sørge for, at jeres MDM-løsning understøtter elementer, der er tilknyttet funktionen Mistet, f.eks. afsendelse af mistet-besked, anmodning om enhedens placering og genaktivering af funktionen Mistet efter nulstilling eller gendannelse. Bemærk, at funktionen Mistet giver en administrator tilladelse til at få oplyst den mistede enheds placering, selvom brugeren har slået lokalitetstjenester fra.

Automatisk indstilling af enheder

Med tilmeldingsordningen for enheder (DEP) får I en hurtig og effektiv metode til implementering af hospitalsejede iOS-enheder, der er købt direkte hos Apple eller autoriserede Apple-forhandlere og udbydere, som deltager i ordningen. Med DEP kan I automatisk tilmelde patientenheder til MDM ved aktivering. I kan også tilmelde iOS-enheder manuelt til DEP ved hjælp af Apple Configurator 2, uanset hvor I har købt dem. Med DEP er enhederne altid overvåget, og MDM-tilmelding er obligatorisk. Brugeren har dog en midlertidig periode på 30 dage til at fjerne enheden fra tilmelding, overvågning og MDM.

Konfigurer DEP-indstillinger

Tilknyt enheder i DEP til jeres MDM-løsning, og overvej at bruge følgende indstillinger:

- Slå overvågning til.
- Tillad pardannelse (slå det senere fra i profilen, hvis det er nødvendigt).
- Tillad ikke fjernelse af MDM-profil.
- Kræv MDM-tilmelding.
- Spring alle trin over i Indstillingsassistent.

Bemærk: Beskrivelserne og grupperingen kan variere afhængigt af den konkrete MDM-løsning.

Distribuering af apps

Mængdekøbsordningen (VPP) giver jer mulighed for at købe store partier af apps, der skal distribueres til patienter via jeres MDM-løsning. MDM-løsninger kan integreres med VPP og bruges til at distribuere apps til enheder i alle lande, hvor disse apps er tilgængelige.

Tildel apps til enheder

Både når det gælder implementeringer med opbevaring på stuen og central opbevaring, skal I tildele apps direkte til enheder ved hjælp af jeres MDM-løsning eller Apple Configurator 2. Når en app er blevet tildelt til en enhed, bliver appen sendt til den pågældende enhed via MDM – uden behov for Apple-id eller iTunes-konto. Alle brugere af denne enhed har adgang til appen.

Lav et app-katalog

Det anbefales stærkt, at I samarbejder med leverandøren af jeres MDM-løsning om at lave et katalog over anbefalede apps, som I ønsker, at jeres patienter skal kunne bruge. Et app-katalog præsenterer udvalgte apps, som patienterne selv kan hente efter behov.

Under den indledende indstilling er det normalt kun nødvendigt at have nogle enkelte vigtige apps til patienten installeret på forhånd. Med indførelsen af et app-katalog kan patienterne selv hente andre anbefalede apps efter behov. Det begrænser belastningen af jeres Wi-Fi-netværk og reducerer markant implementeringstiden.

Opbevaring på stuen

Når jeres netværk og MDM-infrastruktur er klar, skal I vælge et implementeringsscenarie. Med opbevaring på stuen kan I indstille enheder og opdatere software trådløst samt automatisk nulstille iPad, når patienten udskrives. Dette implementeringsscenarie gør det muligt at opbevare enheder på stuerne, så patienterne kan tilpasse deres iPad, når de ankommer.

Indledende indstilling

Når patienten modtager en iPad, hjælper den indbyggede Indstillingsassistent vedkommende med at gøre enheden personlig. På velkomstskærmen, hvor der står "Hej", kan patienten vælge sprog, land, "indstil manuelt" og offentligt tilgængeligt Wi-Fi-netværk. Der er ikke behov for andre trin, og de øvrige skærme i Indstillingsassistenten kan springes over via DEP.

For at muliggøre forbindelse og tilmelding fra starten skal I have et offentligt tilgængeligt Wi-Fi-netværk uden brug af en tvungen portal. Når en iPad er tilmeldt, kan MDM automatisk overføre enheden til et privat Wi-Fi-netværk, hvor resten af indstillingen kan udføres. Brug af et privat Wi-Fi-netværk forbedrer desuden sikkerheden gennem hele patientens indlæggelsesforløb.

Herefter konfigurerer MDM enhedens indstillinger og installerer apps trådløst. Processens varighed afhænger af jeres Wi-Fi-netværk, om I bruger Caching Server eller ej og antallet af apps, som I installerer på hver iPad.

Nulstilling af enheden

Når patienten er udskrevet, skal enheden nulstilles til den næste patient, hvilket gøres ved at slette alt indhold og alle indstillinger. I kan enten slette iPad eksternt via MDM eller nulstille enheden manuelt.

Ekstern sletning via MDM

MDM kan udføre ekstern sletning og trådløst fjerne det pågældende indhold fra enheden. Denne opgave vil sædvanligvis blive udført af en IT-administrator, men det er bedre at automatisere den eksterne sletning via jeres MDM-løsning. Når en patient bliver udskrevet, kan I f.eks. udføre en ekstern sletning i en hospitalsindstilling ved at sende en meddelelse fra jeres elektroniske patientjournaler (EPJ) eller et andet journalsystem til jeres MDM-løsning. Dette signal kan bruges til at aktivere en ekstern sletning via MDM-serveren. Det er to forskellige tilgange til at integrere denne proces:

- MDM-leverandører kan programmere koden, så den "lytter" efter en udskrivelseskommando fra et tilgængeligt system eller netværkspunkt og derefter igangsætter en ekstern sletning.
- EPJ-systemer kan have denne funktion indbygget i deres produkter for at automatisere sletning af iPad, så snart en patient bliver udskrevet.

Manuel nulstilling

En medarbejder kan udføre en manuel nulstilling ved at trykke på Indstillinger > Generelt > Nulstil > Slet alt indhold og alle indstillinger.

Bemærk: Hvis I bruger implementering med central opbevaring, er det ikke nødvendigt at slå ekstern sletning til. Læs mere i afsnittet Central opbevaring.

Central opbevaring

Alternativet til opbevaring på stuen er at opbevare flere iPad-enheder på en sikret vogn, hvor de er tilsluttet en transportabel arbejdsstation. Hver iPad er tilsluttet en Mac via USB, og der bruges en automatiseret tilmeldingsproces til at slette og nulstille jeres iOS-enhed til hjemmeskærmen, før den tildeles den næste patient.

Denne arbejdsgang muliggør en håndfri indstillingsproces vha. Apple Configurator 2, så brugerne ikke behøver at trykke på iPad-skærmen, hvilket desuden gør det nemmere for medarbejderne at tjekke iOS-enheder ind og ud.

Indstilling af Apple Configurator

Med dette gratis macOS-program kan I opdatere iOS-enheder til den nyeste version af iOS, konfigurere enhedsindstillinger og -begrænsninger samt installere apps og andet indhold. Efter den indledende indstilling kan I administrere det hele eksternt vha. MDM eller Apple Remote Desktop. Læs mere i afsnittet Installation af Apple Remote Desktop.

I kan få flere oplysninger om, hvordan man opretter og eksporterer en "supervision identity" i Apple Configurator 2, på http://configautomation.com/identity-files.html. Denne identitet skal uploades i MDM og bruges til overvågning af DEP-tilmeldte enheder.

Aktivér værktøjer til automatisering

Automator bruges til at automatisere funktioner fra macOS og styresystemets programmer. Automator-handlinger til Apple Configurator 2 gør det nemt at oprette og anvende automatiseringsinstrukser (automation recipes) til indstilling af iOS-enheder. Det betyder, at du nemmere kan konfigurere og indstille flere tilsluttede iPad-enheder. Se https://configautomation.com for flere oplysninger om brug af Automator.

Sørg for, at "Install Automation Tools" er slået til i Apple Configurator 2 ved at vælge Apple Configurator 2 > Install Automation Tools.

Opret en Wi-Fi-konfigurationsbeskrivelse

Brug Apple Configurator 2 til at oprette en konfigurationsbeskrivelse med Wi-Fi-oplysninger. Beslut, om følgende skal bruges:

- SSID (Service Set Identifier)
  - Skjult netværk (Hidden Network)
  - Automatisk tilslutning (Auto Join)
- Indstilling af proxy (Proxy Setup)
- Sikkerhedstype (Security Type)
- Adgangskode (Password)
- Netværkstype (Network Type)

Udfør indledende tilmelding af enhed

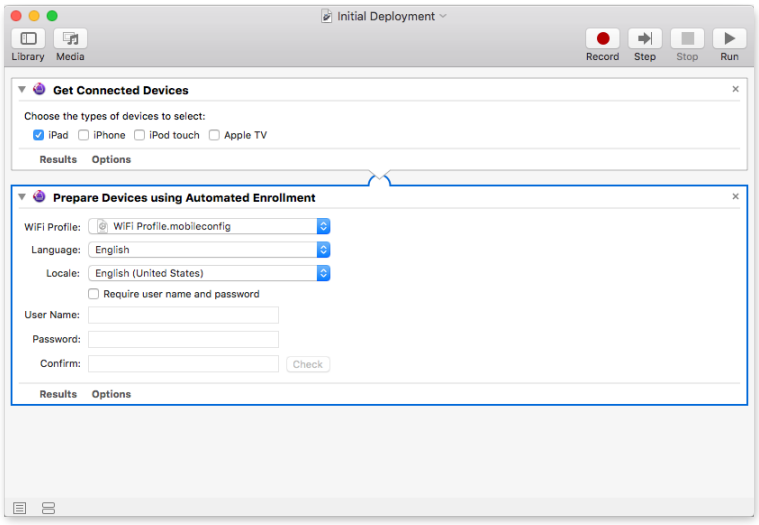
Opret følgende arbejdsgang for at udføre en indledende tilmelding af enheder. I Apple Configurator 2 er DEP-tilmelding tilgængelig som en Automator-handling.

Get Connected Devices: Vælg typer af enheder, der skal vælges.

Prepare Devices using Automated Enrollment: Tilføj den tidligere oprettede Wi-Fi-konfigurationsbeskrivelse, og angiv indstillinger for sprog og sprogvariant.

Bemærk: Apple Configurator 2 skal køre for at forhindre, at iTunes og Fotos starter under tilslutning af enheden. Det kan alternativt forhindres ved at bruge standardkommandoer.

Slut alle enheder til iPad-vognen eller USB-hubben, og kør den indledende implementeringsarbejdsgang.



Konfigurer Automator til at opdatere enheden

Opret følgende arbejdsgang for at udføre opdatering af enheden ved tilslutning af en iPad. Hent og installer følgende tilføjelseshandlinger fra http://configautomation.com/attach-workflow.html.

Automator-arbejdsgang: En tilføjet arbejdsgang skal begynde med handlingen "Begin Attached Workflow" og slutte med handlingen "End Attached Workflow".

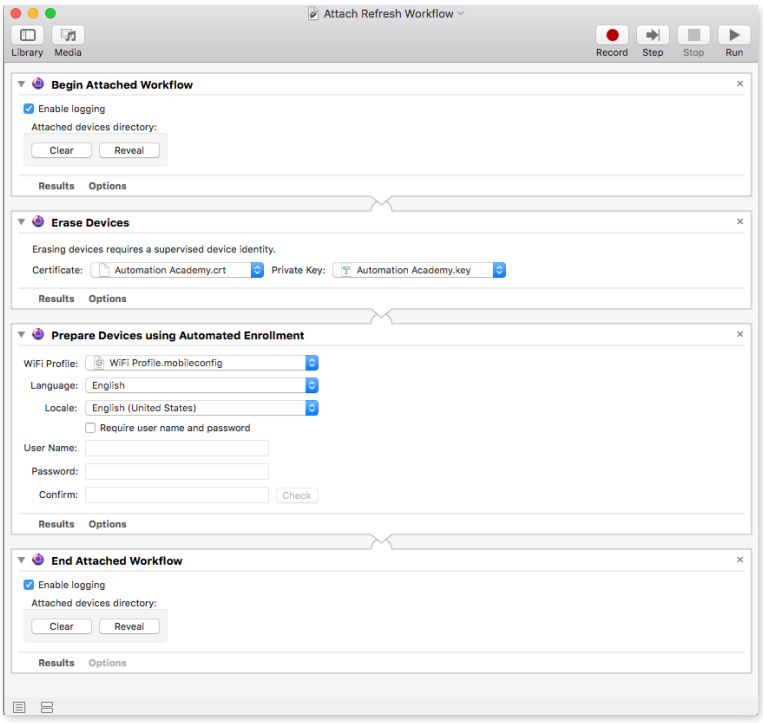
Handlingerne Slet (Erase) og Gendan (Restore): Den første handling efter "Begin" vil enten være "Erase Devices" eller "Restore Devices".

Handlingen Slet enheder (Erase Devices) kræver, at den tilsluttede enhed enten er ulåst og parret eller overvåget. Der kræves en supervision identity for enheder, der ikke har iOS 9 eller nyere.

Hvis den tilsluttede enhed ikke opfylder disse krav, eller den installerede supervision identity i Apple Configurator 2 ikke er i overensstemmelse med den identitet, der bruges til at overvåge enheden, udføres arbejdsgangen ikke.

Handlingen "Restore" kræver ikke, at enheden er overvåget. Den sletter brugerindholdet på den tilsluttede enhed og installerer det nyeste styresystem, hvis det er nødvendigt. Denne proces tager ca. fem minutter.

Prepare Devices using Automated Enrollment: Konfigurer denne handling på samme måde som den indledende konfiguration.



Tilføj kommandofil med shell-script

Der skal oprettes en kommandofil med shell-script, hvis arbejdsgangen automatisk skal gennemføres ved tilslutning af iOS-enhed. Dette script køres af cfgutil-programmet. Yderligere oplysninger findes på http://configautomation.com/attach-workflow.html. Se nedenstående eksempel:

```
    #!/bin/bash
    # set attachPID to Process ID of THIS thread
    export attachPID=$$
    # Set Attached Device Directory Value
    workflowPath=$(echo ~/Library/Workflows/attachment-workflow.workflow)
    automator -i
      "ECID=$ECID&attachPID=$attachPID&PATH=$PATH&UDID=$UDID&dev
      iceName=$deviceName&deviceType=$deviceType&buildVersion=
      $buildVersion&firmwareVersion=$firmwareVersion&locationID=
      $locationID" "${workflowPath}"
    # Check if Cache File exists
    if [ ! -f ~/Library/Caches/com.apple.configurator.AttachedDevices/
    $ECID.plist ];
      then
      echo "Cache file not found - Automator Workflow completed
      successfully"
    else
      # Cache file found - Need to check if the PID matches
      echo "Cache File Found - Test PID"
      # Get the PID from the file
      filePID=$(defaults read ~/Library/Caches/com.apple.configurator.
         AttachedDevices/$ECID.plist attachPID)
      if test $attachPID -eq $filePID
      then
      # The file was created by this PID so the Workflow Failed - Clean up
      echo "PID Match - Workflow has failed - Clean up"
      rm ~/Library/Caches/com.apple.configurator.AttachedDevices/
      $ECID.plist
    else
      # Re-Entry - Do Nothing
      echo "Re-Entry - Do Nothing"
    fi
fi
```

I kommandofilen (attach.command) skal I ændre eksempelfeltet til stien til den Automator-arbejdsgang, som I ønsker at køre ved tilføjelse af en enhed:

workflowPath=$(echo ~/Library/Workflows/attachment-workflow.workflow)

Gem dette script sammen med den tilføjede arbejdsgang, og sørg for, at den kan køres (chmod +x).

Forhindring af utilsigtede konsekvenser: Hvis I bruger handlingen "Restore Devices", slettes indholdet på enhver enhed, der tilsluttes arbejdsstationen – uden varsel.

For at begrænse udførelsen af scriptet til kendte enheder kan I tjekke, om den tilføjede enhed er på en liste over enheder, som scriptet genererer.

Få mere at vide i afsnittet Specifying Workflows for Device Groups på http://configautomation.com/attach-workflow.html.

Automatisk opdatering af enheder

Opret og installer en Launch Services-instruktionsfil for at køre det angivne shell-script automatisk, når en iOS-enhed tilsluttes eller frakobles værtscomputeren. Hent eksempelfilerne på http://configautomation.com/autoloaunchfiles.zip.

I den genererede Launch Services-egenskabsliste (com.example.attached.plist) kan I ændre stien i eksempelfeltet til den kommandofil, som I bruger. Efter ændringen skal egenskabsliste-filen gemmes i LaunchAgents-mappen i brugerens Bibliotek-mappe. Processen bliver automatisk indlæst ved næste login, eller den kan slås til/fra manuelt vha. launchctl-kommandoen. I kan finde flere oplysninger på http://configautomation.com/attach-workflow.html. Nedenstående er et eksempel:

```
<?xml version="1.0" encoding="UTF-8"?>
      <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//
EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
   <key>KeepAlive</key>
   <true/>
   <key>Label</key>
   <string>com.example.attached</string>
   <key>ProgramArguments</key>
   <array>
         <string>/usr/local/bin/cfgutil</string>
         <string>-vvv</string>
         <string>exec</string>
         <string>-a</string>
         <string>'/Users/yourUserName/path/to/
         exampleattachment.command'</string>
   </array>
   <key>RunAtLoad</key>
   <true/>
</dict>
</plist>
```

Filtilladelser for overvågningsfiler

For at cfgutil-værktøjet kan bruge overvågningscertifikatet og den private nøgle, må de kun kunne læses af den bruger, der kører scriptet.

I Terminal skal I bruge chmod 700 /path/to/file for at sikre, at denne indstilling er korrekt, hvis overvågningsfilerne er blevet flyttet i filsystemet.

Installation af Apple Remote Desktop

Apple Remote Desktop er et macOS-program til fjernadministration af skrivebordet. Det kan bruges til distribution af software, administration af materialer og ekstern hjælp. Hvis I bruger implementering med central opbevaring, giver Apple Remote Desktop mulighed for at administrere flere arbejdsstationer med Apple Configurator 2 fra en enkelt Mac. På den måde kan I hurtigt foretage nødvendige opdateringer af jeres konfigurationsbeskrivelser uden at afbryde hospitalets medarbejdere i deres arbejde med at tjekke iPad-enheder til patienter ind og ud. Tag en eksisterende pakke, enten fra Apple eller en tredjepart, og brug Install Package til at kopiere og installere ændringer på flere arbejdsstationer i jeres hospitalsmiljø. Med funktionerne til skærmdeling i Apple Remote Desktop kan I yde øjeblikkelig hjælp til eksterne stationer, hvilket sparer tid for både jer og hospitalets personale.

På http://www.apple.com/remotedesktop/pdf/ARD3_AdminGuide.pdf kan I læse mere om indstilling af Apple Remote Desktop.

Opsummering

I har mulighed for at implementere og administrere iPad-enheder til patientbrug, uanset om jeres hospital implementerer iPad til en gruppe af brugere eller på tværs af hele organisationen. Og ved at vælge de rigtige implementerings-strategier for jeres organisation kan I hjælpe jeres personale med at holde fokus på det vigtigste – at tage sig af patienterne.