Sdílené úlohy pro zabezpečení systému a dat

4535 616 18002 Rev A

Srpen 2013

PHILIPS

Philips Ultrasound

22100 Bothell-Everett Highway
Bothell, WA 98021-8431
USA
Telefon +1 425-487-7000 or 800-426-2670
Fax +1 425-485-6080
www.healthcare.philips.com/ultrasound

Obsah

Úvod

Cílem tohoto průvodce je pomoci zdravotnickým zařízením pochopit, jak může být ohrožena bezpečnost ultrazvukových systémů Philips, softwarových produktů a dat pacientů, a zdůraznit úsilí společnosti Philips při zajišťování preventivní ochrany proti narušení bezpečnosti.

Tento dokument se týká bezpečnosti ultrazvukových systému a softwaru QLAB a Q-Station na hostitelských počítačích. Jsou-li ultrazvukové systémy Philips dodány jako kompletní s omezením na autorizované a dostupné položky, pak jsou hostitelské počítače QLAB a Q-Station dodány, nakonfigurovány a spravovány zdravotnickým zařízením nebo jednotlivci.

Bezpečnostní zdroje ultrazvukového systému, jako jsou např. bezpečnostní bulletiny, FAQ a informace o slabých místech, získáte na webu věnovaném bezpečnosti produktů společnosti Philips na adrese:

www.philips.com/productsecurity

Obecné informace

Následující obecné informace se vztahují k zabezpečení ultrazvukových systémů Philips, softwaru QLAB, Q-Station a dat pacientů.

- Ultrazvukové systémy Philips nepodporují operace s relacemi více uživatelů. Jsou navrženy jako zařízení pro jednoho uživatele. Přístup v rámci klinického použití přes síť není podporován, s výjimkou aplikací autorizovaných společností Philips.
- Ultrazvukové systémy a softwarové produkty QLAB a Q-Station nejsou určeny k dlouhodobému ukládání dat. Trvalá data pacientů je nutno archivovat v systému PACS nebo dočasně ukládat na výměnná média (viz „Výměnná a přenosná média“ na straně 13).
- Ultrazvukové systémy se prostřednictvím funkce operačního systému XP Embedded nebo Windows Embedded Standard 7 automaticky spouští do vlastní schránky. Tím jsou splněny požadavky na bezpečnost lékařských zařízení, které vyžadují, aby byly ultrazvukové systémy provozuschopné co nejdříve po zapnutí. Přístup k operačnímu systému má pouze autorizovaný personál společnosti Philips.

- Softwarové produkty QLAB a Q-Station se zavádějí na pracovní plochu, kde uživatel následně spouští příslušnou aplikaci.
- Systém se nesynchronizuje s centrálními administrativními systémy uživatelských účtů zákazníka (například LDAP, Active Directory).

Kontrola slabých míst zabezpečení ultrazvukových systémů Philips

Philips se zaměřuje na pomoc všem zákazníkům při udržování důvěrnosti, neporušenosti a dostupnosti dat pacientů a zajištění svých ultrazvukových systémů při průběžném vytváření a spravování těchto informací s maximální bezpečností. Ultrazvukové systémy mohou být bezpečnostně zranitelné, jsou-li připojeny do sítě nebo pokud přijímají data z přenosných médií.

Strategie hloubkové ochrany bezpečnosti

Zabezpečení dat pacientů a produktů Philips proti vnitřnímu i vnějšímu ohrožení ve zdravotnických zařízeních vyžaduje komplexní víceúrovňovou hloubkovou bezpečnostní strategii ochrany informací a systémů (zahrnující směrnice, postupy i technologie).

Konkrétní otázky bezpečnosti týkající se vašeho zařízení konzultujte se specialisty na zabezpečení v těchto úřadech či institucích s odpovídajícím zaměřením:

- Hlavní úřad pro bezpečnost informací
- Úřad pro informace
- Úřad pro utajení a bezpečnost HIPAA (v USA)
- Bezpečnostní úřad

Pokud se chcete obeznámit se všeobecnými bezpečnostními problémy nebo se specifickou zranitelnosti svého ultrazvukového systému, obraťte se na servisního zástupce Philips.

Regulační prostředí

Vývoj a výroba lékařských zařízení podléhají přísné regulaci stejně jako bezpečnost a důvěrnost informací o pacientech u poskytovatelů zdravotní péče. To klade jak na poskytovatele zdravotní péče, tak i na výrobce techniky vysoké nároky, pokud jde o jejich schopnost rychle reagovat na ohrožení bezpečnosti dat pacientů, která jsou uložena v lékařských zařízeních.

Ochrana elektronicky spravovaných informací o zdraví pacientů

Jednou z nejdůležitějších hodnot, vyžadujících ochranu a bezpečnostní opatření, jsou informace o zdravotním stavu pacientů. Dodržování zásad ochrany osobních údajů při zacházení s informacemi o zdravotním stavu pacientů vyžadují například následující předpisy a nařízení, která také tyto bezpečnostní zásady a opatření specifikují:

- Zákon o převoditelnosti a evidenci zdravotního pojištění (HIPAA), USA (www.hhs.gov/ocr/privacy/),
- Evropská směrnice 93/42/EEC o lékařských zařízeních,
- Japonská směrnice HPB517,
- části amerického federálního zákona na podporu ekonomiky (HITECH), formálně známého jako Zákon o americkém zotavení a reinvestování z roku 2009, které se týkají HIPAA.

VAROVÁNÍ

Soubory vnitřních elektronických protokolů vytvořené systémem jako součást normálního provozu obsahují názvy ukládacích složek, a proto budou obsahovat identifikační informace o pacientech, klinických lékařích a dalším personálu, které se používají v názvech těchto složek. V rámci údržby, monitorování nebo oprav, případně úkonů spojených s vývojem a dalšími úkony se vztahem k systému, může společnost Philips získávat, ukládat nebo jinak používat tyto soubory protokolů.

Prevence proti neoprávněným zásahům

Platné předpisy vyžadují, aby Philips i ostatní výrobci ultrazvukových systémů dodržovali předepsané postupy zajištění kvality, na jejichž základě se ověřují a povolují modifikace jejich systémů. Z důvodu zajištění správné funkčnosti systému je operátorům a majitelům systémů umožněno provádět pouze takové zásahy, které schválí Philips.

VÝSTRAHA
Neprovádějte změny v nastavení konfigurace ultrazvukového systému, pokud k tomu nejste vyškoleni autorizovaným servisním zástupcem Philips. Změny systémových nastavení, jako je konfigurace DICOM, jsou přípustné pouze za dodržení přísných pravidel. Nekompetentní zásahy mohou být příčinou nesprávné funkce systému a mohou vést ke stanovení chybných diagnóz.

VAROVÁNÍ
Některé ultrazvukové systémy Philips jsou dodávány ve stavu „bezpečném ve výchozím nastavení“. Pokud uživatel bezpečné nastavení poruší, společnost Philips nenese odpovědnost za zajištění bezpečného a efektivního provozu systému.

VAROVÁNÍ
Bez souhlasu zástupce Philips neinstalujte na ultrazvukový systém software. Nekompetentní instalací softwaru můžete způsobit nesprávnou funkci systému.

Role společnosti Philips v partnerství pro produktovou bezpečnost

Philips působí celosvětově na základě politiky produktové bezpečnosti, kterou je řízena tvorba výrobků podle zásad bezpečnosti konstrukce, hodnocení rizik a incidenční odezvy na zjištěná slabá místa dosavadních produktů. Philips zavedl celosvětový postup sledování problémů a má stále širší přehled o bezpečnostních problémech týkajících se systémů Philips.

Náprava slabých míst

Útvar produktových specialistů společnosti Philips průběžně sleduje výskyt nových slabých míst v zabezpečení našich systémů, včetně těch, která se projeví se softwarovými produkty třetích stran, těch, která zjistí smluvní prodejci systémů, i těch, která jsou hlášena z jednotlivých zdravotnických zařízení.

Celosvětová síť pracovních skupin zaměřených na informace zpětné vazby o bezpečnostních incidentech produktů shromažďuje a spravuje informace a adresy zranitelných míst, která ovlivňují produkty Philips. Tyto skupiny trvale rozšiřují své aktivity v úsilí celosvětově podchytit všechny systémy.

Cílem každé skupiny je zhodnotit každé reálné i potenciální narušení bezpečnosti s jasným zhodnocením rizika, ohrožení či zranitelnosti a podle potřeby vytvořit plán opatření k nápravě zjištěného slabého místa, který zahrnuje vymezení a komunikační postupy. To znamená, že Philips jednak informuje zákazníky o slabých místech systému, a zároveň vyvíjí a realizuje opatření k potlačení rizika. Více informací o slabých místech systému naleznete na této webové stránce:

www.philips.com/productsecurity

Konstrukční zdokonalení

Philips pro identifikaci potenciálních slabin aktivně provádí interní bezpečnostní hodnocení produktů. Na základě těchto informací často konstruktéři Philips stanovují konfigurační a konstrukční změny, kterými systém posilují vůči vnějšímu ohrožení. Z těchto informací se pak stávají požadavky na bezpečnost při vývoji nových produktů. Politika produktové bezpečnosti Philips vyžaduje, aby záměry konstrukční bezpečnosti byly součástí vývoje každého nového produktu.

Role společnosti Philips v partnerství pro produktovou bezpečnost

Praktické zavádění technických bezpečnostních prvků je závislé na místě a podmínkách realizace a může využívat řadu technologií jako jsou firewally, antivirový software, technologie ověřování přístupu atd. Jako všechny počítačové systémy i ultrazvukové systémy vyžadují ochranu obvykle poskytovanou firewally a dalšími bezpečnostním prvky mezi vlastním lékařským systémem a systémy přístupnými z vnějšku. Agentura U.S. Veterans Administration pro tento účel vyvinula široce využívanou architekturu pro izolaci. Tento okruh a síťové ochranné prvky jsou základem dobrého zabezpečení v praxi. *Příručku k architektuře izolace lékařských zařízení oddělení Veterans Affairs* naleznete na těchto webových stránkách:

www.himss.org/files/HIMSSorg/content/files/MedicalDeviceIsolationArchitectureGuidev2.pdf

Obecná situace

Společnost Philips nepodporuje zdravotnická zařízení v instalaci softwaru třetích stran (například antivirových programů, kancelářského softwaru, systémových aktualizací, firewallů apod.) na ultrazvukové systémy, pokud společnost Philips předem instalaci neschválila. Zásahy do systému Philips prováděné neoprávněně ruší záruku a mohou být příčinou nesprávné funkce systému. Servisní zákroky vyvolané takovými zásahy nespadají pod působnost servisní smlouvy se společností Philips. Protože nekompetentní zásahy mohou ovlivnit funkci a bezpečnost systémů nepředvídatelným způsobem, nezodpovídá společnost Philips za chování zařízení, na němž byl proveden zásah bez jejího souhlasu.

Reakce na bezpečnostní problémy s produktem a zjištění malwaru

V případě bezpečnostního problému s produktem nebo v případě, že zjistíte přítomnost malwaru (škodlivého softwaru) v systému, ihned systém odpojte od sítě a nahlaste událost servisnímu zástupci společnosti Philips. Případně nahlaste událost odesláním e-mailu na adresu productsecurity@philips.com.

Pokud v systému zjistíte přítomnost malwaru, neinstalujte ani nespouštějte software třetích stran, jako jsou např. antivirové programy, pro detekci a odstranění malwaru. Pokud je na systému zjištěn malware, jediným bezpečným obnovením je obnovení systému z obrazu disku, které provede servisní zástupce společnosti Philips.

Bezpečnostní problémy a doporučení

Následující pokyny ukazují konkrétní příklady zranitelnosti systému i dat a metody pro poskytnutí ochrany.

Bezpečnost v síti

Ultrazvukový systém připojený k síti musí být připojen k bezpečné místní síti, která poskytuje ochranu proti počítačovým virům a jiným škodlivým programům a komunikačním prostředkům. Zabezpečte svoji místní síť příslušnými ochrannými prostředky, jako jsou používání pouze zabezpečených bezdrátových technologií, brána firewall, systémy ochrany proti průnikům a prevence průniků a sledování slabých míst.

Servisní síť na dálku

Společnost Philips vytvořila celosvětovou internetovou síť, která umožňuje propojit ultrazvukové systémy a některé softwarové produkty s moderními servisními zdroji. Servisní síť na dálku (RSN) společnosti Philips poskytuje bezpečnou komunikační infrastrukturu, která umožňuje kterékoliv z následujících připojení:

- Internet-based Secure Sockets Layer Link (iSSLLink),
- Virtual Private Network (VPN).

Sofistikované bezpečnostní prvky optimalizují ochranu sítí, lékařských systémů a osobních údajů pacientů.

Při dálkovém spojení se sítí RSN se používá explicitní autorizace a autentizace spojení a technologie šifrování dat. Společnost Philips veškeré datové přenosy do místa zákazníka i z něj šifruje pomocí šifrovacích protokolů 3DES (Triple Data Encryption Standard) a AES (Advanced Encryption Standard). Protokoly 3DES a AES jsou v souladu s americkými federálními standardy pro šifrování datových přenosů.

Servis na dálku společnosti Philips je vytvořen tak, aby udržel vysokou úroveň ochrany důvěrných lékařských informací. Ve většině případů může zástupce servisního oddělení společnosti Philips dokončit servisní úlohu prozkoumáním technických údajů z daného systému, aniž by měl přístup k osobním datům. Ve vzácných případech, kdy analýzu a opravu nelze provést bez přístupu k osobním datům, je přístup umožněn pouze školenému a autorizovanému personálu společnosti Philips.

Další informace naleznete v brožuře *Zabezpečení dálkově poskytovaných služeb společnosti Philips*, kterou si můžete stáhnout z webových stránek Zabezpečení dálkově poskytovaných služeb:

www.healthcare.philips.com/main/support/equipment-performance/remote-services/security.wpd

Aktualizace antivirového programu

Antivirový software vnáší do ultrazvukových systémů společnosti Philips ohrožení zabezpečení a výkonu a přináší málo pozitiv. Jako alternativní řešení společnost Philips nabízí zabezpečení nastavení systému odolné vůči virům, které využívá předem nainstalovanou softwarovou bránu firewall nebo které minimalizuje vystavení síťových portů a služeb nežádoucímu riziku. Také internetové prohlížeče nejsou v ultrazvukových systémech Philips dostupné ani potřebné.

Tato opatření značně snižují hrozbu virů. V kombinaci s účinnými zásadami zabezpečení sítě je riziko virové infekce systému Philips minimální (viz „Antivirová kontrola a aktualizace“ na straně 18).

Fyzická kontrola přístupu

Každé zdravotnické zařízení musí fyzický přístup k ultrazvukovému systému omezovat, aby předešlo nežádoucím úmyslným i neúmyslným kontaktům s neoprávněnými osobami. Přístupnost místnosti s ultrazvukovým systémem musí být kontrolována předepsaným postupem identifikace osob oprávněných ke vstupu a pobytu v daném prostoru. Informace o opatřeních či postupech pro kontrolu přístupu do příslušného prostoru mohou poskytnout odborníci na zabezpečení a bezpečnost práce.

Umístění monitorů

Nežádoucí vizuální přístup ke chráněným informacím lze minimalizovat takovým umístěním systémového monitoru, kterým se zamezí viditelnosti obrazovky z chodby, ode dveří a jiných míst.

Společnost Philips neustále vylepšuje zabezpečení svých produktů, což zahrnuje také nové ovládací prvky, které umožňují šetřiči obrazovky chránit informace před prohlížením, potřebuje-li uživatel od systému odejít.

Před ponecháním zařízení bez dohledu po jakkoli dlouhou dobu odstraňte obsah obrazovky odhlášením systému nebo ručním vymazáním.

Ochrana přihlášením a odhlášením uživatele

Ultrazvukové systémy Philips, které jsou založeny na technologii Windows XP Embedded, nepoužívají technologii Windows Logon. Přístup je zajištěn přes vlastní schránku prostřednictvím funkce operačního systému XP Embedded nebo Windows Embedded Standard 7. Uložené chráněné informace o zdravotním stavu (PHI) jsou před neoprávněným přístupem chráněny heslem, zatímco bezpečnostní předpisy pro zařízení jsou plněny tolik, aby bylo zařízení co možná nejvíce provozuschopné.

U systémů, které to umožňují, je dobrým bezpečnostním ochranným prvkem důsledné vyžadování jména uživatele a přístupového hesla. V obou případech musí kontrolu přístupu zajistit samotné zdravotnické zařízení.

Ochrana přihlašování a zabezpečení heslem zahrnuje:

- Zavedení silných hesel. To je pro zvýšení bezpečnosti nejjednodušší a nejúčinnější metoda. Bezpečná hesla by měla sestávat z nejméně osmi alfanumerických znaků, obsahovat jak malá a velká písmena, tak i číslice a speciální znaky, jako například „@“ či „*“. Nikdy nepoužívejte slova, která lze nalézt ve slovníku.
- Neposílejte uživatelská jména a hesla poštou.
- Pravidelně hesla měňte.

Zajistěte, aby si operátoři systému osvojili návyk odhlašovat systém bezprostředně po dokončení práce.

Výměnná a přenosná média

Ultrazvukové systémy Philips umožňují exportování výsledků klinických vyšetření na výměnná média, včetně disků CD a DVD a zařízení připojitelných prostřednictvím rozhraní USB. Vyjímatelná nebo přenosná média se snadno ztratí nebo poškodí a existuje u nich riziko technologické zastaralosti. Společnost Philips doporučuje, abyste nepoužívali vyjímatelná nebo přenosná média pro dlouhodobé skladování dat pacientů. Místo toho ukládejte data pacienta na systém PACS nebo jiná média pro dlouhodobé ukládání. Pro účel použití vyjímatelných nebo přenosných médií dodržujte doporučené postupy vašeho IT oddělení.

VAROVÁNÍ
Před použitím jakéhokoliv média v ultrazvukovém systému nebo pracovní stanici je dobré používat pouze média z důvěryhodných zdrojů a provést vyhledávání virů, aby bylo zajištěno, že neobsahují viry nebo trojské koně, které by mohly infikovat počítače. Informace o softwarovém zabezpečení naleznete v části „Bezpečnostní ochranný software“ na straně 17.

VAROVÁNÍ
Výměnná média obsahující snímky nebo jiné zdravotní informace musí být uchovávána na bezpečném místě, do kterého nemají přístup nepovolané osoby.

VAROVÁNÍ
Systémová rozhraní pro komunikaci s výměnnými médii nelze deaktivovat.

POZNÁMKA
Některé ultrazvukové systémy obsahují nastavení, které zabraňuje exportu na vyměnitelná média.

Při používání výměnných médií (paměťových zařízení typu flash, disků CD a DVD, paměťových zařízení USB a magnetooptických disků) mějte na paměti tato bezpečnostní rizika:

- Ultrazvukové systémy mohou být bezpečnostně zranitelné, pokud jsou u nich používána vyjímatelná média. Z výměnného média se mohou do systému dostat viry. Společnost Philips doporučuje, abyste úložné zařízení USB před použitím v systému naformátovali.
- Výměnná média obsahující data pacientů jsou ohrožena přístupem nepovolaných osob.
- K zamezení neoprávněného přístupu k datům o pacientech je třeba vyřazená datová média ničit.
- Systém neprovádí šifrování osobních dat, která jsou uložena na systémovém pevném disku nebo exportována na výměnná média.

Příklad uchovávání informací

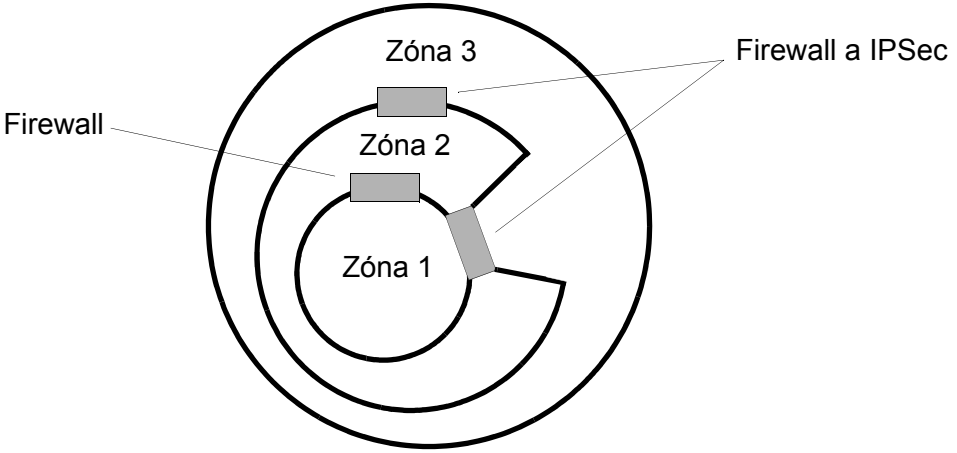
Tento příklad ukazuje, jak dodržovat zásady bezpečnosti informací v zónovém modelu informačního toku.

Požadavky na prostředí

Konfigurace ultrazvukových systémů je založena na předpokladu, že zdravotnické zařízení zabezpečí jejich provozní prostředí ochrannými mechanismy síťového přístupu, šifrováním a sledováním zranitelných míst či napadení. Udržování bezpečnosti ultrazvukového systému v bezpečném prostředí dále vyžaduje, aby jakoukoliv aktualizaci systémového softwaru prováděl oprávněný zástupce Philips, pokud Philips sám neurčí jinak.

Informační zóny

Model informačních toků je obvykle součástí bezpečnostních standardů. Jednoduše lze tento model znázornit schématem členění zdravotnického zařízení na tři zóny (viz obrázek), kdy každá zóna má rozdílná uživatelská práva a přístup k informacím. Některá zařízení neumožňují v nejširší zóně přístup k informačnímu systému vůbec, neboť nejsou schopna zajistit jejich ochranu a neporušenost.



Řešení pro zajištění bezpečnosti mezi zónami

Zóna 1: Oddělení ultrazvuku

Většina přenosů snímků se uskutečňuje v rámci Zóny 1. Zálohy, kopie a disky se snímky DICOM musí personál oddělení spravovat pečlivě.

Zóna 2: Ostatní části zdravotnického zařízení

Zóna 2 zahrnuje všechna ostatní oddělení, která mají přístup k systému a v některých případech k internetu. Důsledná kontrola přístupu a průběhu činnosti je kriticky důležitá.

Zóna 3: Internet

Zóna 3 je užívána pro spojení se servisem na dálku.

Bezpečnost mezi zónami

Bezpečnost mezi zónami se zajišťuje standardními prostředky zabezpečení výpočetních systémů. Vedení musí znát předpokládaný rozsah systémového provozu, aby se volbou správných zabezpečovacích prostředků vyhnulo vzniku úzkých míst v informačních tocích. Přenosy obrazových souborů (snímků) vyžadují širokopásmové síťové kanály.

Bezpečnost uvnitř zón

Na bezpečnosti uvnitř zón se podílejí jak standardní prostředky zabezpečení výpočetní techniky, tak bezpečnostní funkce ultrazvukového systému.

Bezpečnostní ochranný software

Tento oddíl uvádí informace o bezpečnostním softwaru a softwaru třetích stran pro ultrazvukové systémy Philips.

Philips poskytuje ověřené aktualizace softwaru pro zabezpečení operačního systému a v některých případech i antivirovou ochranu. Tyto aktualizace poskytují trvalou ochranu provozuschopnosti ultrazvukového systému a zabezpečení proti bezpečnostním hrozbám.

POZNÁMKA
Aktualizace jsou poskytovány prostřednictvím pravidelného vydávání nových verzí a prostřednictvím postupu Philips Field Change Order.

Aktualizace bezpečnosti operačního systému

Philips hledá a ověřuje aktualizace operačního systému, které mohou chránit bezpečnost slabých míst, a začleňuje je do nových verzí softwaru pro své ultrazvukové systémy. Podle potřeby jsou v době mezi plánovaným vydáním jednotlivých verzí poskytovány opravné verze softwaru (aktualizace operačního systému) pro nápravu poznaných slabin. Tyto aktualizace smí instalovat pouze oprávněný servisní zástupce společnosti Philips. U některých systémů vám může být povoleno instalovat aktualizovaný software vlastními silami, pokud je vám tento poskytnut společně s příslušnými pokyny oprávněným servisním zástupcem společnosti Philips. Máte-li se společností Philips uzavřenu platnou servisní smlouvu, může společnost Philips provádět také přímou dálkovou instalaci aktualizovaného softwaru do ultrazvukového systému.

Díky prodlouženému životnímu cyklu ultrazvukových systémů Philips je možné, že operační systém ultrazvukového systému dosáhne stavu ukončení podpory společnosti Microsoft před plánovaným datem ukončení podpory ultrazvukového systému. Aby poskytovala pokračující ochranu vašemu systému a mohla tak prodloužit podporovatelnost operačního systému, udržuje společnost Philips se společností Microsoft rozšířené smlouvy o podpoře. K zajištění pokračující bezpečnosti výrobků Philips přijala společnost Philips mnohá bezpečnostní opatření, jak je uvedeno v tomto dokumentu a v dokumentech k jednotlivým výrobkům. V kombinaci s efektivní politikou síťové bezpečnosti se tak vytváří obranná strategie, která může významně zvýšit dlouhou životnost a podporovatelnost vašeho ultrazvukového systému Philips při současné minimalizaci rizik pro integritu dat a zákaznické sítě.

Antivirová kontrola a aktualizace

Ultrazvukové systémy Philips se liší stupněm přístupnosti a ochrany proti ohrožení virovou infekcí. V každém případě je pro zdravotnické zařízení nejlepší ochranou proti virům vytvoření účinných zásad bezpečnosti provozu sítě.

Philips pracuje na tvorbě bezpečné konfigurace různých systémů různými způsoby. Pro některé systémy povoluje Philips instalaci antivirového softwaru. Do jiných systémů může Philips začlenit softwarový firewall nebo jako součást bezpečnostní architektury omezit síťový přístup k portům a službám. Philips také ověřuje, hodnotí a instaluje aktualizované verze softwaru ultrazvukových systémů, kterými eliminuje poznaná slabá místa softwaru. Kombinací těchto opatření s účinnou strategií síťové bezpečnosti zdravotnických zařízení je riziko napadení softwaru těchto systémů virovou infekcí významně redukováno.

Zjistíte-li výskyt malwaru ve svém systému, neprodleně se obraťte na příslušného autorizovaného servisního zástupce společnosti Philips.

Zálohy a archívy

Postup při zálohování dat

Ultrazvukové systémy nejsou určeny k tomu, aby byly používány k trvalému ukládání citlivých osobních informací. Takové informace je vždy nutno co nejdříve přenést do vhodného paměťového zařízení.

Celý ultrazvukový systém nelze zálohovat. Abyste zajistili bezpečné a efektivní uchovávání a ukládání záznamů o pacientech a informací o konfiguraci systému, připojujte systém za účelem ukládání a duplikace dat k jiným systémům (například k systému PACS nebo k pracovní stanici PIC).

Ultrazvukové systémy jsou určeny k uchování informací pouze v případech, kdy je to nezbytné k sestavování externí dokumentace pro zdravotní záznamy (například filmů, grafických schémat a vytisknutých záznamů). Je-li nezbytné dodatečné zálohování, vytvořte před odstraněním záznamů administrativní protokol pro archivaci všech klinických vyšetření.

Pravidelně zálohujte soubory s výsledky softwaru QLAB a Q-Station a exportovaných snímků a uchovávejte kopie těchto záloh jinde než na serveru.

Úplné informace o připojování k externím systémům a o zálohování systémových souborů naleznete v uživatelské příručce ke svému ultrazvukovému systému.

Plány obnovy po havárii

Je vaší povinností zkontrolovat, že váš plán obnovy po havárii zahrnuje pravidelné a kompletní zálohy dat pacienta. Ultrazvukové systémy jsou zařízení pro nesouvislé ukládání dat; data pacienta je třeba z ultrazvukového systému exportovat. Ujistěte se, že vytváříte také zálohu specifických nastavení systému. Další informace o exportu dat pacienta a vytváření záloh nastavení systému naleznete v informacích pro uživatele ultrazvukového systému. K vytváření záloh dat pacienta exportovaných ze softwaru QLAB a Q-Station používejte zálohovací software.

Zabezpečení dat pro procesy Off-Cart

Data lze exportovat z ultrazvukového systému za účelem archivace, kvantifikace nebo distribuce. Každé zdravotnické zařízení je zodpovědné za zajištění kompletní ochrany informací pacienta před neautorizovaným přístupem.

Data pacienta lze exportovat různými způsoby: archivovacím mechanismem ultrazvukového systému, exportem přes DICOM, exportováním obrazu nebo exportováním hlášení.

Data lze přesunout pomocí sítě nebo výměnných médií jako disky CD, DVD a disky USB.

Informace a snímky pacienta ze systému QLAB a Q-Station jsou šifrovány a jsou přístupné prostřednictvím softwaru operačního systému Windows. Ujistěte se, že dodržujete správné bezpečnostní zásady a konfigurace hostitelského počítače QLAB a Q-Station a jeho prostředí, včetně médií pro čtení, sítě, aplikací třetích stran, zálohovacích souborů a opatření zamezující přístup nepovolaných osob.

Ověření uživatele

Ujistěte se, že hostitelské počítače produktu QLAB a Q-Station jsou nastaveny na ověřování uživatele a že jednotlivci používající hostitelské počítače produktu QLAB a Q-Station mají uživatelské jméno a heslo. Tyto informace můžete použít k ochraně dat ve složkách a jednotlivých souborech.

K přístupu k hostitelským počítačům a údajům QLAB a Q-Station používejte neuhodnutelná hesla. Další informace o heslech naleznete v části „Ochrana přihlášením a odhlášením uživatele“ na straně 13.

Operační systém

Ujistěte se, že operační systém a aplikace na hostitelských počítačích QLAB a Q-Station obsahují aktuální opravy, aktualizace a inovace.

Konfigurace sítě

Je-li hostitelský počítač QLAB nebo Q-Station připojen k místní síti, měla by tato síť být nastavena tak, aby poskytovala ochranu proti počítačovým virům a jiným škodlivým programům a komunikačním prostředkům. Zajistěte, aby místní síť používala odpovídající ochranu, jako jsou používání pouze zabezpečených bezdrátových technologií, firewally, systémy pro detekci narušení a vyhledávače virů.

Přístupnost souboru

K ovládání přístupu k souborům, které obsahují data pacienta, na hostitelských počítačích QLAB a Q-Station použijte vlastnosti zabezpečení souborů operačního souboru.

Zabezpečení sdílené složky

Výchozí nastavení zabezpečení sdílené složky umožňuje všem uživatelům zobrazit a měnit obsah složky. Nachází-li se ve sdílených složkách data pacienta, ujistěte se, že jsou provedená vhodná bezpečnostní nastavení. Jednotlivým uživatelům nebo skupinám uživatelů můžete přiřadit práva.

POZNÁMKA
Přenos obrazů jiných než DICOM z ultrazvukového systému SONOS do systému PACS vyžaduje bezpečnostní nastavení otevřené sdílené složky.

Antivirová ochrana

Abyste zajistili ochranu hostitelských počítačů QLAB a Q-Station, přidružených sítí a výměnných médií před viry a podobnými softwarovými hrozbami, používejte aktuální antivirový program a systém pro ochranu před neoprávněným vniknutím.

Další informace o použití výměnných a přenosných médií ke sdílení informací naleznete v části „Výměnná a přenosná média“ na straně 13.

Opravné aktualizace systému

Architektura ultrazvukového systému nepodporuje provádění opravných aktualizací pomocí softwaru, který lze stahovat prostřednictvím internetu. Společnost Philips spravuje plošné aktualizace s ověřenými bezpečnostními vylepšeními prostřednictvím autorizovaných vydání softwaru.

Vzdálená správa

Je-li na hostitelském počítači QLAB nebo Q-Station používána vzdálená správa, ujistěte se, že je nastavena na zabezpečenou vzdálenou správu.

Ochrana dat pacienta

Přenos dat pacienta mezi ultrazvukovým systémem a hostitelským počítačem QLAB nebo Q-Station může vést k riziku odhalení dat pacienta. Ujistěte se, že data jsou během přenosu zabezpečená.

Jedním ze způsobů bezpečného přenosu je server QLAB DICOM. Informace o aplikaci serveru QLAB DICOM naleznete v příručce *Uživatelská příručka produktu QLAB*.

Po provedení exportu dat z QLAB Q- Apps (zásuvných modulů plug-in) otevřete složku Q-App (nachází se v instalační složce produktu QLAB **Philips\QLAB\Results**) a nastavte bezpečnostní oprávnění omezující přístup k souborům a složkám na základě ověření uživatele.

Přenos dat DICOM

Standardní soubor DICOM není šifrován, ale k přečtení šifrovaných dat v souboru DICOM je nutná softwarová aplikace rozpoznávající DICOM. Jakmile však data ze stanice Q-Station exportujete, proveďte odpovídající kroky, které omezují přístup k těmto datům.

Skrytí dat pacienta v prohlížečích souborů QLAB

Chcete-li zabránit zobrazování dat pacienta v okně **File Open**, použijte k jejich zobrazení formát **List** a sloupce obsahující příslušná data pacienta zmenšete tak, aby byl jejich obsah skryt. Další informace o použití okna **File Open** aplikace QLAB naleznete v uživatelské příručce k produktu QLAB.

Export dat ze softwaru QLAB a Q-Station

K ochraně dat exportovaných ze softwaru QLAB a Q-Station použijte odpovídající bezpečnostní opatření.

Produkt Q-Station obsahuje funkce „anonymizace“, která v případě, že je použita při exportu dat pacienta na disk CD, DVD nebo do složky systému Windows, některé atributy pacienta nahradí anonymními hodnotami.

VAROVÁNÍ
Exportovaná data nejsou ve výchozím nastavení anonymizována. Jsou-li data exportována do systému nebo úložného zařízení, které není chráněno heslem nebo jiným způsobem, jsou přístupná všem uživatelům. Jste zodpovědní za zajištění toho, že soukromí pacienta nebude při exportu narušeno.

Export obrazů

Software QLAB snímky exportuje pouze tehdy, je-li v nastaveních aplikace QLAB vybrána možnost **Hide Patient Data**.

Export výsledků kvantifikace

Než provedete export výsledků kvantifikace ze softwaru QLAB, ujistěte se, že je v nastaveních vybrána možnost **Hide Patient Data**. Tato volba zabrání zobrazení důvěrných dat pacienta v souboru s výsledky.

Hodnoty dat v souborech exportovaných ze softwaru QLAB a Q-Station nejsou vůči změnám uzamčeny. K ochraně dat použijte vlastnosti zabezpečení souborů proti zápisu.