MEDAX Systems s.r.o.
Oběžná 2075/11, 709 00 Ostrava, Česká Republika
Tel.: +420 733 398 440
mail: podpora@medax.cz ,URL: www.medax.cz
Společnost vedená u Krajského soudu v Ostravě,
spisová značka C 30978

Zabezpečení osobních dat

Informační systém SmartMEDIX (dále Systém) vyžaduje určité podmínky pro běh z hlediska bezpečnosti dat a nabízí řadu možností jak bezpečnost dat posílit.

Zajištění prostředí

Výchozím prostředím pro běh Systému je počítač nebo vnitřní síť počítačů s aktuálně podporovaným a aktualizovaným operačním systémem Windows společnosti Microsoft. Komplementem operačního systému je zajištění zabezpečení systémové ochrany vhodným prostředkem, zjednodušeně antivirem.

Systém pro svůj chod vyžaduje:

a) PC s vícejádrovým procesorem o taktu minimálně 1.5GHz.
b) Operační paměť minimálně 2GB, lépe více.
c) Volný diskový prostor v řádu minimálně GigaBajtů (optimálně disk SSD).
d) Běžící databázový server Firebird nebo MS SQL Server v aktuálně podporované verzi;
e) Zabezpečený přístup k internetu (náležitě konfigurovaný a zaheslovaný router a další síťové prvky), náležité zabezpečení WI-FI sítě, je-li používána.

Technická a organizační opatření

Základním opatřením je zabezpečení přístupu do prostor a k IT technice. Velmi důležitá je rovněž ochrana uživatelského účtu operačního systému Windows náležitým heslem. Vhodným opatřením je šifrování svazku či oddílu, na kterém Systém běží a jsou uchovávána data.

Aktualizace Systému

Systém má ve výchozím stavu nastavenou automatickou on-line aktualizaci při uvolnění nové verze. Průběžná aktualizace systému je nezbytná z hlediska vývoje zabezpečení a legislativy.

Agenda přístupů

Systém nabízí řízení přístupu k datům v horizontální rovině řízením přístupu k položkám dokumentace a ve vertikální rovině řízení přístupu k jednotlivým záznamům.

Systém řeší zabezpečení dat těmito opatřeními:

a) Nutnost definice náležitě silného hesla pro přístup do Systému. Heslo musí být minimálně sedmiznakové, obsahovat velká i malá písmena a číslo nebo znak.
b) Základní rozdělení přístupu je rozšířený administrátorský přístup vs. uživatelský běžný přístup. Právo administrátor lze přiřadit jednotlivým uživatelům. Běžný uživatel nemá přístup do řady konfigurací vyhrazených pouze pro administrátora.
Upozornění: není-li administrátor nastaven, mají všichni uživatelé právo administrace (případ jednoho uživatele nebo velmi malé ambulance). V případě práce více uživatelů by měl být administrátor vždy nastaven.
c) Definice organizační struktury s hierarchií Zařízení [, Oddělení], Pracoviště, Personál. Uživatel se hlásí na příslušnou úroveň personálu a prováděné operace jsou zaznamenávány vzhledem k této úrovni.
d) Lze nastavit tato globální práva pro jednotlivé uživatele:
- KONTAKT: právo vidět a použít pro výstup kontaktní údaje;

MEDAX Systems s.r.o.
Oběžná 2075/11, 709 00 Ostrava, Česká Republika
Tel.: +420 733 398 440
mail: podpora@medax.cz ,URL: www.medax.cz
Společnost vedená u Krajského soudu v Ostravě,
spisová značka C 30978

- EXPORT: právo tisknout a exportovat;
- STATUS: právo vidět stavové informace v zápatí aplikace.

e) Na úrovni personálu lze nastavit vertikální omezení přehledů. Omezení přístupu lze definovat např. na možnost vidět jen daným personálem pořízená data nebo vidět přehledová data jen přihlášeného pracoviště, oddělení, zařízení atp.

f) Možnost nastavení horizontálních přístupových práv k položkám dokumentace prostřednictvím definice profilu práv a přiřazení daného profilu jednotlivému personálu. V praxi tak lze rozlišit role uživatelů v Systému, např. recepce, sestra, lékař apod.

g) Sdílení dokumentace umožňuje definovat dokumentační jednotky a přiřadit tyto jednotlivým pracovištím. Lze tak dosáhnout stavu, kdy pracoviště nebo skupina pracovišť odbornosti A pracuje a vidí svá data, které nevidí pracoviště ostatních odborností a naopak.

h) Soukromí/VIP je možnost skrýt data vybraných pacientů/klientů respektive řídit přístup k těmto datům pro jednotlivé uživatele. První uživatel-koordinátor, který si nastaví přístup k danému pacientovi/klientovi, se stává správcem a může přidávat oprávnění pro další uživatele.

Zálohování

Je nutno pravidelně zálohovat data na oddělený zabezpečený prostředek tak, aby bylo eliminováno riziko technického selhání, kybernetického útoku či odcizení počítače. Jako optimální se jeví každodenní zálohování.

Další opatření k posílení zabezpečení

Audit zabezpečení

Audit zabezpečení je nástroj analyzující nastavení Systému s identifikací rizikových či nedostatečně ošetřených míst.

Automatické uzamykání systému

Automatické uzamčení systému je vhodné řešit na úrovni systému Windows, aby nemohlo dojít k nežádoucí manipulaci s počítačem. Systém nabízí uzamykání, které lze nastavit v Konfigurace/Aplikace/Zabezpečení počtem minut, po kterém se při nečinnosti uzamkne.

Nezobrazení záznamů bez filtru v kartotéce

Výchozí zobrazení kartotéky je zobrazení pacientů s příjmením od A. Není úplně žádoucí, aby se záznamy pacientů z počátku kartotéky zobrazovaly po každém spuštění bez filtru. Systém nabízí nastavení *Nezobrazit záznamy pacientů, není-li zadán filtr (nezobrazit záznamy z počátku kartotéky)* v Konfigurace/Aplikace/Zabezpečení. Nadále zůstává, že si Systém ukládá posledně zvolený filtr kartotéky a při příštím zobrazení tento filtr použije (analogie záložky v knize).

Chráněná repozitoř

Výchozím uložením obrazových dat a velkých textů je sdílená složka (chráněná heslem). Vyšší úroveň zabezpečení velkých dat nabízí Chráněná repozitoř, kterou lze nastavit v Konfigurace/Aplikace/Obrazová dokumentace. Repozitoř je implementována databází a k jednotlivým datovým objektům tak není přímý přístup. Chráněnou repozitoř lze dále zálohovat na cloud prostřednictvím volitelné nadstandardní služby.

MEDAX Systems s.r.o.
Oběžná 2075/11, 709 00 Ostrava, Česká Republika
Tel.: +420 733 398 440
mail: podpora@medax.cz ,URL: www.medax.cz
Společnost vedená u Krajského soudu v Ostravě,
spisová značka C 30978

Šifrování úložiště databáze

V rámci eliminace rizika zneužití dat při odcizení technicky je vhodným opatřením ochrana databáze i dalších souborů prostřednictvím šifrování. V systému Windows lze toto zabezpečení realizovat nástrojem BitLocker (ve verzi Professional či vyšší).

Nastavení náležitě silného administrátorského hesla pro přístup k databázi

Vždy je nutno nastavit dostatečně silné heslo pro administrátorský přístup a v žádném případě neponechávat výchozí heslo. Pokud na databázovém serveru běží i jiné systémy (zvací systémy, analyzátory, zobrazovací zařízení apod.), je nutno provést změnu hesla v součinnosti s dodavateli těchto systémů, aby nedošlo k omezení funkčnosti.

Při použití databáze Firebird je administrátorský účet SYSDBA.

Při použití databáze MsSQL Server je administrátorský účet dán buď autentifikací systému Windows, na kterém databáze běží, nebo administrátorským účtem (typicky sa) při ověřování samotným MsSQL serverem.

Ing. Marek Dobiáš

Digitálně podepsal Ing. Marek Dobiáš
Datum: 2020.11.26 16:35:06 +01'00'