Deloitte.

Řešení pro automatickou detekci podezřelých událostí

Zdravotní pojišťovny

Září 2013

Obsah

Centrum excelence pro střední a východní Evropu

- Oddělení aplikované analytiky a forenzních služeb slouží jako centrum excelence pro střední a východní Evropu. Oddělení slouží sdílí své zkušeností a znalostí v rámci regionu na poli pokročilých analytických řešeních, forenzních služeb, implementaci řešení pro automatickou detekci podezřelého jednání apod. Úzce spolupracuje s ostatními centry excelence po světě při vývoji nových produktů a určování nových trendů v oboru.
- Pro podporu své činnosti využívá vlastní datové laboratoře s výkonnou výpočetní technikou. Laboratoř má je držitelem certifikace ISO 27001 (bezpečnost informací)

Datově analytická laboratoř v Praze

Úvod do detekce podezřelých událostí

Trápí zdravotní pojišťovny podvodné jednání?

Pojištěnci více kontrolují své zdravotní účty, někteří odhalí podvod

Tuzemské zdravotní pojišťovny se shodují na rostoucím zájmu svých klientů o kontrolu jejich osobních účtů. Například Česká průmyslová zdravotní pojišťovna (ČPZP) zaznamenala dokonce dvojnásobný nárůst oproti loňsku. Ačkoli údaje ve výpisech většinou souhlasí, našlo se již několik případů, kdy pacient takto odhalil podvodnou činnost.

Zdroj: Novinky.cz

Mrtvé duše po česku: Podvody lékařů nikdo neřeší

Praha - Českým zdravotnictvím ročně zbytečně proteče zhruba 20,1 miliardy korun, vyplývá z nedávno zveřejněných odhadů Transparency International.

Zdroj: Aktualně.cz

Podvody lékařů můžete odhalit sami. Požádejte o výpis zdravotní péče

Zkontrolujte si svého lékaře, vyzývají zdravotní pojišťovny. Někteří doktoři totiž pojišťovnám účtují náklady za výkony, které ve skutečnosti vůbec neprovedli. Výpis z účtu pojištěnce lze získat zdarma a je možné, že i vás nakonec překvapí, jaké zdravotní péče se vám v uplynulém roce údajně dostalo.

Zdroj: Novinky.cz

Špinavý boj vrcholí. Zdravotní pojišťovny si přetahují klienty

Blíží se konec června, tedy uzávěrka přestupu mezi zdravotními pojišťovnami. Zprostředkovatelé za provizi očerňují konkurenční pojišťovny a děsí klienty ztrátou zdravotní péče. Loni pojišťovnu změnilo 144 tisíc lidí. Zdravotní pojišťovny lákají klienty na nicotné výhody. Ze zákona přitom nemohou nabídnout ani víc, ani méně než zajištění zdravotní péče.

Zdroj: Idnes.cz

Proč zlepšovat detekci podezřelých událostí?

- Organizace s vyspělou detekcí podezřelých události dokáží lépe bojovat proti externím podvodům a riziky s nimi spojenými. To se odráží především na nákladech s těmito riziky spojenými. Absence efektivního systému detekce přináší nejčastěji tyto hrozby:
  - Kontroly spoléhají často na lidský činitel, efektivitu a preciznost lidské práce.
  - Nově vznikající způsoby podvodu nemusí být pokryty současným systémem kontrol: kontroly musí reagovat na změny systému.
  - Kampaně či nařízení ze strany organizace mohou vycházet na zkreslených údajů. Nově vznikající kampaně a nařízení by již od začátku měli uvažovat opatření na detekci podvodného jednání.
  - Bez efektivních kontrol je obtížné prokázat regulátorovi, že systém boje proti podvodnému jednání je funkční. To pak vrhá špatné světlo na práci interního auditu.
  - V systému kontrol je třeba zohlednit i mimořádné výkyvy na trhu.
- **Organizace s kvalitním detekčním systémem mají:**
  - Výbornou pozici pro detekci podvodů a jejich následným prokazováním.
  - Při odhalení podvodů mohou tyto organizace efektivně využít informace zjištěné v rámci vyšetřování těchto událostí. A to pro detekci obdobných existujících případů a dále zamezit jejich přehlédnutí v budoucnu.
  - Zvýšení efektivity vynakládaných prostředků za nakupované služby.
  - Minimalizace finančních dopadů podvodů a dopadů na reputaci organizace.

Proč jsou páchány podvody?

- Pohnutky k páchání podvodu jsou různé, téměř vždy se však drží těchto zásad:
  - Co možná nejnižší riziko odhalení
  - Minimální náročnost provedení
  - Maximální možný osobní profit (zisk)
- Druh podvodu (pojišťovny obecně):
  - 17% vymyšlené pojistné plnění (neexistence pojištěné události)
  - 64% nadhodnocení pojistného plnění

Zdroj: Asociace německý pojišťoven (GDV), 2002

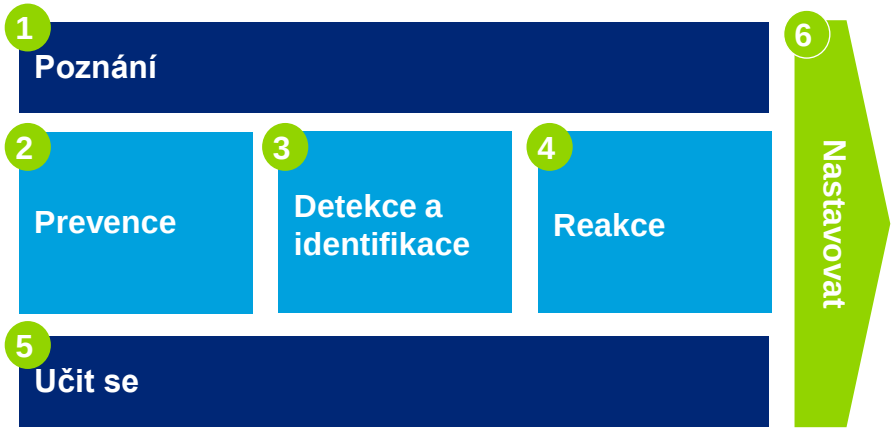
- Poznatky z behaviorální ekonomie:
  - I inteligentní a dobře vychovaní lidé začnou podvádět, jakmile jim k tomu dáme příležitost. A to ne způsobem „několika zkažených jablek v úrodě“, ale spíše většina začne podvádět jen trošku.
  - V případě, že v systému jsou nahrazeny peníze za body/žetony (i s možností jejich přímé směny za peníze) roste výskyt podvodného jednání až dvojnásobně

Zdroj: Dan Ariely: Predictably Irrational, 2008

Úvod do detekce podezřelých událostí

Přístup Deloitte

Přístup společnosti Deloitte se skládá z přístupu založeného na 6 krocích, složených ze samotné implementace a soustavného vylepšování systému, tak aby systém maximalizoval účinnost preventivních opatření, detekce a následné odezvy vůči podvodnému jednání.



1. **Poznání**
   - Sdílení vědomostí a poznatků napříč odděleními
   - Výměna zkušeností vyšetřovatelů a návrh úpravy pravidel
2. **Prevence**
   - Zavádění samokontrolních mechanizmů
   - Medializace odhalených případů dokazujících efektivitu kontrol
3. **Detekce a identifikace**
   - Pomocí prediktivní analytiky vytvořit set pravidel a systémů kontrol jak identifikovat podezřelé jednání a monitorovat ho
   - Definovaní managementu podezřelých událostí a procesu vyšetřování
4. **Reakce**
   - Sestavení podrobných reportů s auditním záznamem dokazující podvodné jednání, jasná identifikace stop
   - Podpora v rámci soudních sporů nebo uzavírání nových smluv
5. **Učit se**
   - Vytvoření každoročního přehledu detekovaných událostí a použitých kontrol
   - Analýza významu jednotlivých kontrol a významu různých typů podvodů
6. **Nastavovat**
   - Aktualizace procesů, kontrol a technologií
   - Rozvoj tréningu a školení

Detekce podezřelých událostí ve zdravotnictví

Fáze 1 – Poznání 1/2

Využití vlastního know-how organizace

V organizacích existuje know-how jak detekovat podezřelé případy a ověřit, zda se jedná o podvod či nikoliv. Tyto vědomosti jsou však často roztříštěny v týmech, či nejsou vhodně popsané. Z toho důvodu se díváme na historické případy, tehdy dostupné informace a výstup – tedy to jak byly vyhodnoceny pověřenou osobou. Na základě toho dokážeme připravit set pravidel podle skutečného chování a rozhodování těchto osob. Tato generovaná pravidla slouží jako podklad do diskuze, jak by měla vypadat výsledná pravidla pro automatickou detekci.

Analýza historických případů

- Identifikace tehdy dostupných informací k danému případu a výsledek rozhodnutí.
- Hledání rozhodovacích pravidel za pomoci již definovaných pravidel (revize postupu rozhodování) tak s využitím metod pokročilé analytiky.
- Jako podklad slouží velké množství případů, zpravidla 80-90% dostupných.

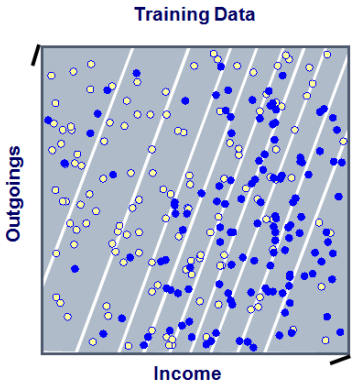
Stanovení nových pravidel

- Prezentační vrstva ukazující efektivitu jednotlivých pravidel a vztah mezi dostupnými informace.
- Nalezení slabých míst v informačních zdrojích.
- Diskuze na definicích nových pravidel a rozhodovacích stromů.

Fáze 1 – Poznání 2/2

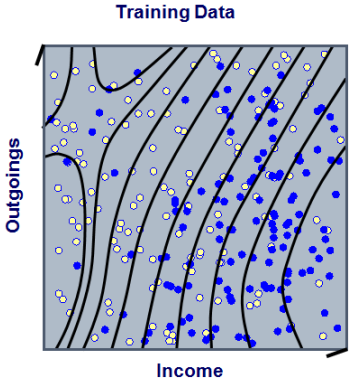
Pokročilé metody na hodnocení chování subjektů a jejich klasifikace

Tradiční přístupy modelování chování či segmentace jsou mnohdy nepřesné a neefektivní, protože nejsou schopny obsáhnout anomálie specifických subjektů



- Tradiční přístup předpokládá většinou lineární charakter, např.:
  - Větší subjekt ➔ více bodů
  - Speciální činnost ➔ více bodů
  - Celkový počet bodů je výsledné hodnocení subjektu
- Používán téměř univerzálně v modelech hodnotící chování subjektů
- Pro doladění je třeba vytvořit velké množství výjimek

Aby bylo možné definovat skutečné chování subjektu, musíme odhlédnout od tradičních lineárních modelů, což jsou typicky modely na vyhledávání neočekávaných změn.



- Zlepšený přístup, který nepředpokládá lineární vztahy
- Dokáže odhalit anomálie
- Nový model dokáže snížit náklady na manipulaci s výjimkami a jejich správu

Fáze 2 – Prevence

Zamezení vzniku podezřelých událostí

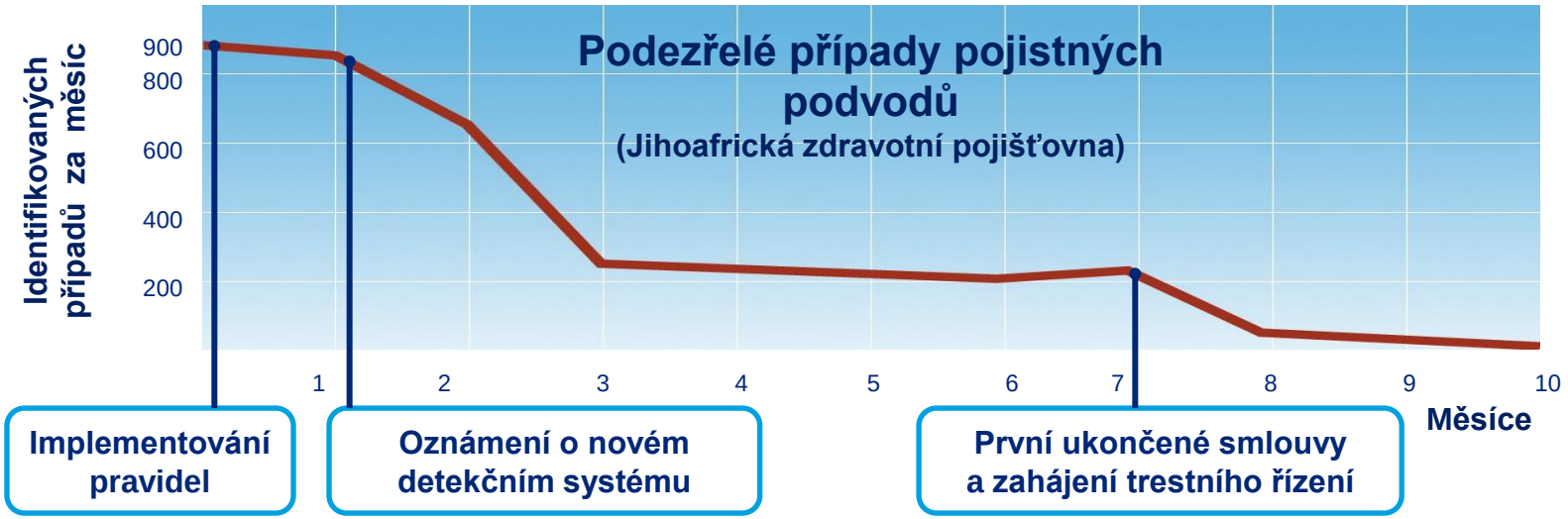
Vhodně nastavený systém preventivních opatření dokáže výrazně snížit vznik podvodného jednání a to především díky strachu z odhalení původce.

Samokontrolní mechanismy

- Například zavedení smluvních podmínek, pokud počet podezřelých/odmítnutých případů dosáhne určité hranice
- Aktivní podpora pojištěnců v hledání neprovedených služeb
- Tvorba interní black-listů problémových subjektů

Medializace odhalených případů

- Zkoumaný subjekt se musí dozvědět, že se zvýšilo riziko případného odhalení podvodného jednání.
- Musí být známy případy potrestání podvodného jednání



Fáze 3 – Detekce a identifikace

Práce s pravidly a výstupy analýz

Za pomoci metod pokročilé prediktivní analytiky je možné v reálném čase aplikovat a vyhodnocovat data za celé portfolio pojištěnců. Hledat specifické závislosti a zároveň upozorňovat vyšetřovatele na detekované podezřelé případy. V rámci investigace se stává, že je nalezeno nové pravidlo, které dříve nebylo uvažováno – z toho důvodu je vítanou funkcí toto pravidlo moci aplikovat i zpětně na starší data.

Uplatňování pravidel	• Doplňování pravidel za chodu a na základě detekovaných událostí • Analýza a detekce událostí v reálném čase • Možnost využití funkcí jako kategorizace, prioritizace, sumarizace / agregace, korelace, apod. • Vyvolání akce na detekovanou událost (např. workflow) • Komunikace s jinými systémy
Parametry pro definování scénářů	• Vybrané objekty (obrazovky / logy nebo části jejich obsahu) • Korelace detekovaných dat • Časová korelace událostí, datum a čas • Původ události • Korelace událostí provedených na různých místech • Agregace výskytů událostí
Oblast pravidel	• Možnost vymezení určitých částí sítě jako nemonitorované či monitorované náhradním způsobem • Možnost definování ignorovatelných forem událostí • Možnost tvorby knowledge base

Fáze 4 – Reakce

Zamezení vzniku podezřelých událostí

Často se setkáváme s tím, že i když už je podezřelá událost správně detekovaná a vyhodnocená, je problematické připravit podklady pro následné kroky. Jedná se například o souhrnný report, výpis veškerých událostí či detail popis práce a postupu vyšetřovatele. Bez řádných pokladů je poté obtíže inicializovat změnu smluvních podmínek či soudní spor. Dále se setkáváme s tím, že citlivá data jsou vyzrazena uživateli z řad zaměstnanců = i tomu lze předcházet.

Forenzní revize aktivit uživatelů – vizuální záznam kompletních relací uživatelů	• Full-textové vyhledávání v zaznamenaných datech • Zaznamenávaná data jsou šifrována a opatřena digitálním podpisem (potenciálně přípustná u soudu) • Záznam o aktivitě jednotlivých uživatelů; jaká data vyhledávají o co se zajímají
Analytika – identifikace událostí v činnosti uživatelů	• Dynamické profilování a vyhodnocování různých subjektů • Nastavení obchodních pravidel (uzpůsobených potřebám klienta) • Generování výstražných zpráv v reálném čase • Možnost zpětného aplikování nových pravidel
Nástroj pro šetření a správu detekovaných případů (case management)	• Správa detekovaných případů, výstražných zpráv a mimořádných událostí • Flexibilní reporting • Řízení parametrů nastavených pravidel, profilování a vyhodnocování

Fáze 5 – Učit se

Pochopení příčin a následků detekční činnosti

V rámci této fáze se díváme na celý proces zpětně z odstupem, abychom dokázali z nabitých zkušeností získat maximum. Revidujeme již nastavený proces, vyhodnocujeme ho a klademe si otázky, jakým způsobem celý proces vylepšit. V rámci této fáze je vhodné revidovat i použitá pravidla a to hlavně z hlediska jejich účinnosti a efektivity jejich správy – například úpravu pravidel, kde potřebujeme příliš mnoho výjimek.

Vytvoření přehledu detekovaných událostí	• Pravidelný reporting o úspěšnosti celého procesu detekce a hodnocení efektivity vynaložených prostředků do tohoto systému. • Souhrnný report umožňující hledání společných znaků detekovaných případů.
Analýza významu jednotlivých kontrol	• Vyhodnocení náročnosti a významu jednotlivých kontrol • Hodnocení efektivity výběru vzorků pro detailní zkoumání či investigaci • Analýza nově vzniklých pravidel a překryvu současných pravidel
Analýza a aktualizace datových zdrojů	• Vyhodnocení spolehlivosti jednotlivých datových zdrojů s cílem zlepšit slabá místa • Analýza informací, které bylo nutné dodatečně získat z externích zdrojů či mimořádným způsobem

Fáze 6 – Nastavovat

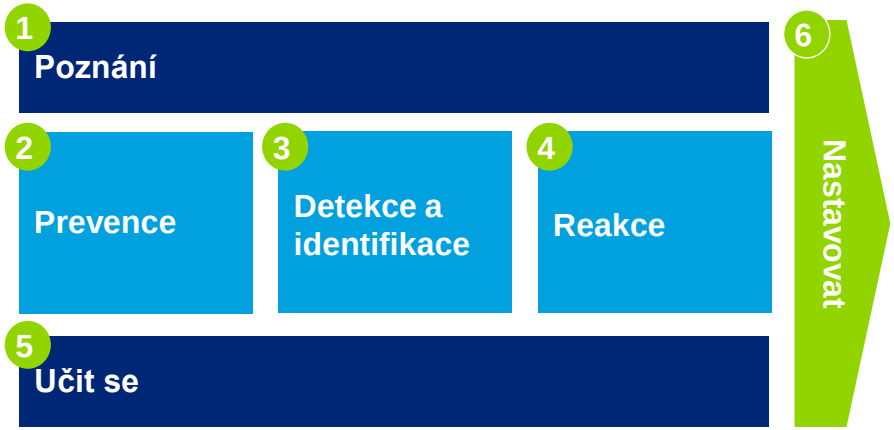
Aktualizace a úprava postupů a pravidel

V této poslední fází se snažíme aplikovat nově získané poznatky a informace ve prospěch vylepšení celého systému. Podklad tvoří předchozí učící se fáze. Klademe důraz jak na aktualizaci samotného detekčního systému tak i na práci s lidskou obsluhou. Zde máme na mysli dodatečné školení v problematických oblastech či školení za účelem lepšího managementu výjimek. Do této fáze také patří případné úpravy motivačního programu zapojených zaměstnanců či úprava jejich pracovních cílů.

Aktualizace pravidel	• Aplikace nově získaných poznatků do nových pravidel. • Odstranění zastaralých pravidel (například kvůli legislativním změnám). • Racionalizace pravidel a tlak na snížení počtu výjimek v nastavení procesu.
Práce s lidskou obsluhou systému	• Rozvoj tréninkových a učebních postupů • Školení pro efektivní management výjimek • Úprava motivačních schémat zaměstnanců. • Nastavování osobních cílů podílejících se zaměstnanců.

Příklady

Příklad – Jak detekovat neprovedené úkony praktických lékařů



1. **Poznání**

   Vycházíme z údajů:
   - Výpis ze zdravotní dokumentace (identifikace lékaře, datum provedení úkonu, typ úhrady, kód diagnózy, popis diagnózy, cena v Kč)
   - Informace o lékaři (vs. ostatní pojištěnci, ordinační hodiny)
   - Informace o pojištěncích (počet a druh návštěv ostatních lékařů)

2. **Prevence**
   - Pojištěnec na vyžádání dostane výpis ze zdravotní dokumentace
   - Pojištěnec může a ví jak hlásit nesrovnalosti

3. **Detekce a identifikace**
   - Pomocí prediktivní analytiky můžeme porovnat strukturu diagnóz, časové rozložení, časový průměr úkonů na jednoho pacienta a porovnat údaje s obdobnými lékaři
   - Můžeme identifikovat vztah pojištěnce k jiným preventivním prohlídkám u ostatních lékařů
   - Výstupem je agregované bodové hodnocení jednotlivých testů → můžeme říci, o jak moc neobvyklý případ se jedná

4. **Reakce**
   - Vyhotovení podrobné reportu s auditním záznamem o daném případy
   - Oslovení pojištěnce kvůli potvrzení či vyvrácení podezřelých úkonů

5. **Učit se**
   - Přehled podezřelých případů během roku a to, zda následná investigace potvrdila či nepotvrdila podvodné jednání
   - Analýza významu jednotlivých kontrol a významu různých typů podvodů

6. **Nastavovat**
   - Úprava testů a pravidel na základě výsledků kontrol s cílem snížit počet chybně hlášených případů

Příklad – Systémové kontroly vykazované péče

Kontrolované oblasti

Věcná správnost

- Zpracování dávky
- Doklad, hlavička dokladu
- Čísla pojištěnců
- Vykazování léků
- Regulační poplatek

Oblast vykazované péče

- DRG
- Diagnóza
- Výkon
- Hospitalizace
- Ambulance

Příklad – Systémové kontroly vykazované péče

Ukázka kontrol pro jednotlivé oblasti

Generování Dávky

- Kontrola **časové souslednosti –** období uzavření dokladu je menší nebo rovno období vyúčtování tohoto dokladu
- Věcná kontrola **souladu položek s číselníkem**, př. položka typ úhrady

Formální, logická správnost dokladu

- Kontrola, zda daný poskytovatel zdravotní péče/ pracoviště tohoto poskytovatele může vykazovat daný **druh dokladu**
- Kontrola zadaného kódu zdravotní pojišťovny **v hlavičce dokladu** a v položkách dokladu

Čísla Pojišťence

- Kontrola, zda datum narození pojištěnce je v souladu s datem narození pojištěnce uvedeném v **Centrálním registru pojištěnců**
- **Formální kontrola** rodného čísla pojištěnce – zda se jedná o číslo neobsahující jiné znaky, zda odpovídá počet znaků atd.

Příklad – Systémové kontroly vykazované péče

Ukázka kontrol pro jednotlivé oblasti

Léky – vykazování

- Kontrola **časové souslednosti –** období uzavření dokladu je menší nebo rovno období vyúčtování dokladu
- Věcná kontrola **souladu položek s číselníkem**, př. položka typ úhrady

Regulační poplatek

- Kontrola **duplicit** vykázání kódu regulačního poplatku na dokladu
- Kontrola **úplnosti** dokladové evidence – existence dokladu regulačního poplatku pro každý vykázaný regulační poplatek

DRG

- Kontrola, zda DRG případ má u hospitalizačního dokladu zadaný správný **kód ukončení** – odlišné kódy dle toho, zda se jedná či nejedná o poslední hospitalizační doklad daného DRG případu

Příklad – Systémové kontroly vykazované péče

Ukázka kontrol pro jednotlivé oblasti

Diagnóza

- Kontrola **pohlaví pojištěnce** – kontrola, zda vykázaná diagnóza je logicky možná u pohlaví pojištěnce
- Kontrola **věku pojištěnce** – kontrola, zda věk pojištěnce je v rozmezí, které stanovuje číselník diagnóz pro danou diagnózu

Výkon

- Kontrola výkonů hrazených **kapitací** – kontrola, zda výkon hrazený kapitačním paušálem není vykázaný zvlášť
- Kontrola **komplexního vyšetření** – opakované kódy komplexního vyšetření u intervalu kratšího než 90 dní u daného poskytovatele zdravotní péče

Hospitalizace

- Kontrola **kódu propustky** – chyba, pokud je kód vykázaný v prvních 3 dnech hospitalizace u pokračující hospitalizace
- Kontrola toho, zda se **nepřekrývá více hospitalizačních dokladů** v rámci jednoho poskytovatele zdravotní péče

Příklad – Systémové kontroly vykazované péče

Ukázka kontrol pro jednotlivé oblasti

Ambulance

- Kontrola, zda na pojištěnce není vykázána **hospitalizace ve stejném období**, kdy je vykazována ambulantní péče
- Kontrola data na **žádance**, zda není vyšší než datum provedení výkonu

Závěr

Shrnutí přínosů

Komplexní dohledování

- Efektivní systém je komplexní - využívá externí a interní zdroje dat, databázi dříve řešených případů
- Vyhodnocování dat z různých systémů najednou
- Hledání souvislostí v chování pojištěnců i poskytovatelů zdravotnických služeb

Pokročilá správa pravidel

- Snadná tvorba pravidel a jejich úprav za účelem snížení planých poplachů
- Profilování na základě analýzy skutečného chování subjektů
- Aplikování nových pravidel na již zaznamenaná data (zpětné dohledávání)

Podpora prevence

- Důraz na rychlou a tvrdou reakci při nalezení podezřelého případy
- Implementace samokontrolních mechanizmů

Podpora auditu

- Zpětné přehrávání zaznamenaných dat
- Auditní záznam pro podporu schopný obstát i u soudních sporů
- Generování výstražných oznámení v reálném čase (zasílání e-mailů)

Kontaktní osoby

Jan Balatka, senior manažer
Tel.: +420 246 042 370 | Mobile: + 420 731 450 902
E-mail: jbalatka@deloitteCE.com

Expert v oboru informačních technologií, zejména informační bezpečnosti, datových analýz a E-Discovery. V současnosti vede týmy Data Analytics, E-Discovery a Continuous Controls Monitoring a je vedoucím laboratoře Deloitte pro analytické a forenzní služby poskytované ve střední a západní Evropě.

Petr Hanuška, senior konzultant
Tel: +420 246 042 870 | Mobile: + 420 602 338 748
E-mail: phanuska@deloitteCE.com

Expert v oboru odhalování a vyšetřování podezřelého jednání, datových analýz a E-Discovery. Podílí se na vývoji nových produktů v oblasti Data Analytics, E-Discovery a Continuous Controls Monitoring.

Ivan Foltman, partner
Tel.: +420 246 042 330
E-mail: ifoltman@deloitteCE.com

Vedoucí partner v oddělení řízení podnikových rizik ve společnosti Deloitte Česká republika. Členem Českého institutu interních auditorů a má více než 25 let profesních zkušeností z Austrálie, České republiky a Slovenska.