Ssenari: Səhiyyə Təşkilatında Data Elminin və Böyük Məlumat Analitikasının Təhlükəsizliyinin təmin edilməsi

Tibbi tədqiqatlar, fərdiləşdirilmiş tibb və xəstələrə qulluq üçün məlumat elminə və böyük məlumat analitikasına əsaslanan səhiyyə təşkilatında xəstə məxfiliyinin qorunması və məlumatların bütövlüyünün qorunması təhlükəsizliyin mühüm aspektləridir.

Əlaqədar suallar:

1. Səhiyyə təşkilatı data elmində və böyük verilənlərin analitika mühitində həssas xəstə məlumatlarına icazəsiz girişin qarşısını almaq üçün möhkəm giriş nəzarətlərini və istifadəçi autentifikasiyası mexanizmlərini necə tətbiq edə bilər?

Səhiyyə təşkilatlarının həssas xəstə məlumatlarının icazəsiz girişə qarşı təhlükəsizlik tədbirləri almaq üçün aşağıdakı möhkəm giriş nəzarətləri və istifadəçi autentifikasiyası mexanizmlərindən istifadə edə bilərlər:

1. İstifadəçi kimlik təsdiqləmə: İstifadəçilərin sistemə daxil olarkən özlərini təsdiq etmələri üçün istifadəçi adı və şifrə kimi məlumatların tələb olunması. Şifrələr güclü olmalıdır və düzgün təhlil olunmalıdır.
2. İki faktorlu autentifikasiya (2FA): İstifadəçilərin sistemə giriş zamanı, birinci faktor kimi şifrəni daxil etmələri tələb olunur və ikinci faktor kimi telefonuna göndərilən təsdiqləmə kodunu daxil etməlidirlər. Bu, hesabın daha çox təhlükəsiz olmasını təmin edir.
3. Ehtiyatkarlıq prinsipi: Yalnız sistemə icazəli olan istifadəçilərə məlumatlara giriş vermək. İstifadəçilərin rollara və icazələrə əsasən tənzimlənmiş bir hiearxiya sistemi ilə icazələrin idarə edilməsi.
4. Ehtiyatkarlıq zamanı qeydiyyat tutma: Sistemə girişlər, hər bir istifadəçinin etibarlılığını təsdiq etmək üçün qeydiyyat altına alınmalıdır. Bu sayədə şübhəli girişlər daha asan aşkarlanaraq müdaxilə edilə bilər.
5. Girişə dair sərhədləndirmələr: Sistemə icazəsiz girişləri aşkarlamaq üçün mümkün olan bütün giriş mərhələlərində sərhədləndirmələr tətbiq edilməlidir. Məsələn, müvafiq IP ünvanlarından girişlərə məhdudiyyət qoymaq, müəyyən saat aralığında giriş imkanlarını məhdudlaşdırmaq kimi.
6. Audit jurnalı saxlamaq: Sistemə girişlər, məlumatlara girişlər və digər əməliyyatlar kimi hər hansı bir sistem hadisəsi üçün audit jurnalı saxlamaq. Bu, potensial həssas məlumatlara icazəsiz girişləri aşkarlamaq və istenməyən davranışları izləmək üçün lazımlıdır.
7. Verilənlər şifrələnməsi: Həssas məlumatların saxlanması və göndərilməsi zamanı verilənlərin şifrələnməsi tətbiq edilməlidir. Bu, məlumatların yalnız icazəli şəxslər tərəfindən oxunabiləcəyini təmin edir.

Bu tədbirlər, səhiyyə təşkilatlarının həssas xəstə məlumatlarının təhlükəsizliyini təmin etmək üçün əsaslı bir zəmin yaradacaq. Əlavə olaraq, hər bir təşkilat özünəməxsus təhlükəsizlik və müdafiə protokollarını tətbiq etməli və məlumatların təhlükəsizliyi üçün ən son tədbirləri izləyən bir təhlükəsizlik stratetiyası hazırlamalıdır.

---

2. Məlumat elmində və böyük məlumat analitikası infrastrukturunda saxlama, ötürmə və emal zamanı xəstə məlumatlarını qorumaq üçün hansı şifrələmə üsullarından istifadə edilə bilər?

Səhiyyə təşkilatlarında xəstə məlumatlarının qorunması üçün çeşitli şifrələmə üsullarından istifadə edilir. İstifadə edilə bilən şifrələmə üsulları aşağıdakıları əhatə edir:

1. Simmetrik şifrələmə: Bu üsulda məlumatların şifrələnməsi və deşifrələnməsi üçün eyni şifrə istifadə olunur. Məlumatlar şifrələndikdən sonra yalnız doğru şifrəni bilən şəxs məlumatlara daxil ola bilir. Simmetrik şifrələmə üsulları arasında Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES) kimi məşhur protokollar yer alır.
2. Asimetrik şifrələmə (hərəkətli şifrələmə): Bu üsulda məlumatları şifrələmək üçün iki fərqli anahtar istifadə olunur - ənənəvi açıq anahtar və gizli anahtar. Açıq anahtar məlumatları şifrələmək üçün istifadə olunur və şifrənin açılması üçün gizli anahtar tələb olunur. Bu üsul RSA protokolunda tətbiq edilir və məlumatların təhlükəsiz bir şəkildə göndərilməsi və qorunması üçün effektivdir.
3. Hash funksiyaları: Hash funksiyaları məlumatların bütünlüyünü yoxlamaq üçün istifadə olunur. Məlumatlar hash funksiyasından keçirilir və alınan nəticə ("hash") məlumatın tam şəklindən asılı olaraq təyin edilir. Əgər məlumat dəyişsə, hash dəyişir. Bu, məlumatın inteqrallığını yoxlamaq üçün istifadə olunur və bir çox şifrələmə protokollarında əlavə təhlükəsizlik səviyyəsi təmin etmək üçün istifadə olunur.

Bu şifrələmə üsulları, səhiyyə təşkilatlarında məlumatların qorunmasında və paylaşılmasında təhlükəsizliyin təmin edilməsində önəmli rol oynayır. Ən əhəmiyyətli olanı isə təşkilatların müvafiq təhlükəsizlik standartlarına və qanunvericilik tələblərinə uyğun şifrələmə protokollarını və prinsiplərini seçmələridir.

Səhiyyə təşkilatlarında məlumat elmində və böyük məlumat analitikası infrastrukturunda saxlama, ötürmə və emal zamanı xəstə məlumatlarını qorumaq üçün bir neçə şifrələmə üsulu mövcuddur. İstifadə edilə biləcək şifrələmə üsullarının bir hissəsi aşağıda açıqlanmışdır:

1. Simmetrik şifrələmə: Simmetrik şifrələmədə eyni açıq mətn şifrəyə çevrilmək üçün istifadə edilir. Şifrələmə və deşifrələmə üçün eyni gizli açar (şifrələmə açarı) istifadə olunur. Ən məşhur simmetrik şifrələmə alqoritmlərindən biri AES (Advanced Encryption Standard)dir. Səhiyyə təşkilatları AES kimi güclü simmetrik şifrələmə alqoritmlərindən istifadə edə bilər.
2. Asimetrik şifrələmə: Asimetrik şifrələmə, şifrələmə və deşifrələmə üçün fərqli açarlar istifadə edən bir şifrələmə metodudur. Bu metodda, məlumatı şifrələmək üçün bir açıq açar (şifrələmə açarı) və şifrəni deşifrə etmək üçün fərqli bir gizli açar (deşifrə açarı) istifadə olunur. Ən məşhur asimetrik şifrələmə alqoritmlərindən biri RSA alqoritmidir. Səhiyyə təşkilatları asimetrik şifrələmə üsullarından RSA-nı istifadə edərək məlumatları təhlükəsiz bir şəkildə şifrələyib deşifrə edə bilərlər.
3. Hash funksiyaları: Hash funksiyaları, verilənlərdən sabit uzunlukda bir məlumat qüvvətlənməsi üçün istifadə edilir. Məlumatın daxil olunan məlumatlarından asılı olaraq sabit uzunlukda bir hash dəyəri yaradır. Hash funksiyaları, məlumat tam təsdiqlənməsində və bir məlumatın orijinalliğinin yoxlanılmasında istifadə olunur. Ən məşhur hash funksiyalarından biri SHA-256-dır. Səhiyyə təşkilatları məlumatın tamamının düzgün şəkildə göndərildiyini və qorunduğunu yoxlamaq üçün hash funksiyalarından istifadə edə bilərlər.

Səhiyyə təşkilatları, məlumat elmində və böyük məlumat analitikası infrastrukturunda məlumatların qorunması üçün şifrələmə üsullarından bir və ya bir neçəsindən istifadə edərək məlumatların gizliliyini və məlumat tamamlığını təmin edə bilərlər. Bu, səhiyyə məlumatlarının istifadəsi və paylaşılması üçün təhlükəsiz bir mühit yaratmağa kömək edəcək.

3. Səhiyyə təşkilatı məlumatların məxfiliyini və təhlükəsizliyini qoruyarkən müxtəlif qurumlar üzrə xəstə məlumatlarını təhlil etmək üçün təhlükəsiz çoxtərəfli hesablama və ya federasiya edilmiş öyrənmə yanaşmalarından necə istifadə edə bilər?

Səhiyyə təşkilatları, məlumatların məxfiliyini və təhlükəsizliyini qoruyarkən müxtəlif qurumlar üzrə xəstə məlumatlarının təhlilini həyata keçirmək üçün təhlükəsiz çoxtərəfli hesablama və federasiya edilmiş öyrənmə yanaşmalarından istifadə edə bilərlər.

Təhlükəsiz çoxtərəfli hesablama, fərqli təşkilatlar arasında məlumatları bölüşmək və əməliyyatları həyata keçirmək üçün bir yoludur. Bu yanaşmada, hər bir təşkilat öz məlumatlarını şifrələyir və digər təşkilatlara göndərir. Digər təşkilatlar gələn məlumatları deşifrə edərək üçüncü tərəflərə məxfi məlumatları ifşa etmədən təhlil etmək üçün işləmələri icra edir. Bu yolla, təşkilatlar arasında əlaqələr təhlükəsiz və məxfi qalır.

Federasiya edilmiş öyrənmə isə bir başqa yanaşmadır ki, fərqli təşkilatlar üçün məlumatların bir araya gətirilməsini və birgə öyrənməni təşkil edir. Burada, hər bir təşkilat öz məlumatlarını öyrənmə modelində təhsil edir və sonra bu modeli bir birinə verməklə digər təşkilatlar da öz məlumatlarını əlavə edir. Beləliklə, birlikdəki məlumatlar bir araya gəlir və daha geniş bir öyrənmə modeli formalaşır. Bu yanaşma, təşkilatlar arasında məlumat paylaşımını minimal səviyyəyə endirir və hər bir təşkilatın məlumatlarının məxfiliyini qoruyur.

Bu təhlükəsiz çoxtərəfli hesablama və federasiya edilmiş öyrənmə yanaşmaları, səhiyyə təşkilatlarına, məlumatların müxtəlif qurumlar arasında təhlil edilməsini təmin etmək üçün bir yol təqdim edir. Bu yanaşmalar, məlumat gizliliyini qoruyaraq və qanunvericilik tələblərinə uyğun olaraq, təşkilatlar arasında işbirliyini artırmaq və sağlamlıq sisteminə dair daha geniş bir şəkildə anlayış yaratmaq imkanı verir.

4. Məlumat elmi və böyük məlumat analitikası təhlükəsizliyi kontekstində HIPAA kimi səhiyyə qaydalarına uyğunluğu təmin etmək üçün hansı siyasət və prosedurlar müəyyən edilməlidir?

Məlumat elmi və böyük məlumat analitikası təhlükəsizliyi kontekstində HIPAA (Health Insurance Portability and Accountability Act) tələblərinə uyğunluğu təmin etmək üçün aşağıdakı siyasət və prosedurlar müəyyən edilməlidir:

1. Məlumatların müstəqil olması: Müəyyən bir sistemə daxil olan səhiyyə məlumatları, digər sistemlərdən asılı olmayan və təmsil edən şəxs və ya təşkilatın məlumatına əsaslanan müstəqil bir formada saxlanılmalıdır.
2. Məlumatların şifrələnməsi: Səhiyyə məlumatları və böyük məlumat analitikası təhlükəsizliyi üçün ən yaxşı təhlükəsizlik tədbirlərindən biri məlumatların şifrələnməsidir. Məlumatlar, əgər zərər görülərsə onlardan yararlanmaq imkanını məhdudlaşdıran şifrələnmə metodu ilə təhlükəsiz bir şəkildə saxlanılmalıdır.
3. İstifadəçi hüquqlarının idarə edilməsi: Səhiyyə məlumatlarına girişin idarə edilməsi, yalnız icazəli və tələb olunan şəxslərin bu məlumatlara giriş etməsinə imkan verən siyasət və prosedurlar təyin edilməlidir. Bu, məlumatların yalnız lazım olan personel tərəfindən istifadə olunması və müəyyən bir məqsədə xidmət etməsi məqsədilədir.
4. Həkkə qarşı qoruma: Səhiyyə məlumatlarının və böyük məlumat analitikası infrastrukturunun həkkə qarşı qorunması üçün uyğun təhlükəsizlik tədbirləri təyin edilməlidir. Bu, şəbəkə təhlükəsizliyi, zərərli proqramların tərkibindən müdafiə, zərərli tərəfindən hücumlar və digər potensial təhlükələrə qarşı mübahisəsiz bir mühafizə sisteminin qurulması deməkdir.
5. Audit və monitorinq: HIPAA tələbləri çərçivəsində, səhiyyə məlumatlarının və böyük məlumat analitikasının təhlükəsizliyini təmin etmək üçün audit və monitorinq prosedurları təyin edilməlidir. Bu, sistemdəki giriş və çıxışların izlənməsi, potensial təhlükələrin və həkkə cəhətdən təhdidlərin aşkarlanması və qarşı tədbirlərin alınması məqsədilə etibarlı bir audit trail sistemi qurulması deməkdir.

Bu siyasət və prosedurlar, səhiyyə məlumatlarının və böyük məlumat analitikasının təhlükəsizliyinin təmin edilməsi və HIPAA tələblərinə uyğunluğunun yaxşılaşdırılması üçün əsaslı addımlar olaraq hesab edilir. Bunlar, müəyyən bir şəxsiyyət məlumatlarının intizamının qorunması, məlumatlara girişin idarə edilməsi, həkkə qarşı təhlükəsizlik tədbirləri və sistem monitorinqi kimi ən vacib aspektləri əhatə edir. Məlumatların və sistemlərin təhlükəsizliyini təmin etmək üçün səhiyyə müəssisələrinin bu siyasət və prosedurlara əməl etməsi əhəmiyyətlidir.

5…. Səhiyyə təşkilatının məlumat elmi və böyük məlumat analitikası mühitində məlumat pozuntularını və ya icazəsiz fəaliyyətləri aşkar etmək və qarşısını almaq üçün məlumatların auditi və monitorinq mexanizmləri necə həyata keçirilə bilər?

Səhiyyə təşkilatları məlumat elmi və böyük məlumat analitikası ilə məlumat pozuntularını və icazəsiz fəaliyyətləri aşkar etmək və qarşısını almaq üçün bir neçə məlumat audit və monitorinq mexanizmlərindən istifadə edə bilərlər. Aşağıda bu mexanizmlərə nümunələr verilmişdir:

1. İstifadəçi hüquqlarının nəzarəti: Məlumat pozuntularını aşkar etmək üçün, səhiyyə təşkilatları məlumat sistemlərində istifadəçilərə verilən hüquqları nəzarət altında saxlamaq üçün uyğun tədbirlər almalıdır. Hər bir istifadəçiyə yalnız lazım olan məlumatlara giriş imkanı verilməli və bu girişlərə nəzarət edilməlidir.
2. İcazə və hesabatlılığın təminatı: Məlumat pozuntularını aşkar etmək üçün, səhiyyə təşkilatları məlumat sistemlərində icazələr və hesabatlılıq qaydalarını tətbiq etməlidir. Hər bir istifadəçiyə yalnız lazım olan məlumatlara icazə verilməlidir və hər hansı bir məlumat pozuntusu hallarında hansı istifadəçilərin hansı məlumatlara giriş etdiyi izlənə bilər olmalıdır.
3. Müəyyən edilmiş monitorinq və audit prosedurları: Məlumat pozuntularını aşkar etmək və qarşısını almaq üçün, səhiyyə təşkilatları monitorinq və audit prosedurları təyin etməlidir. Bu prosedurlar, məlumatların nəzarət altında saxlanılması, monitorinq edilməsi, mövcud pozuntuların aşkarlanması və bunların araşdırılması, həmçinin icazəsiz fəaliyyətlərin təyin edilməsi və müdafiə tədbirlərinin tətbiqi ilə bağlı addımları özəl bir səviyyədə təmin etməlidir.
4. İndiki məlumat pozuntularını aşkar etmək üçün maşın öyrənmə və analitik texnologiyaları: Səhiyyə təşkilatları məlumat pozuntularını aşkar etmək üçün maşın öyrənmə və analitik texnologiyalardan istifadə edə bilərlər. Bu texnologiyalar, anomaliləri və icazəsiz girişləri aşkar etmək üçün məlumatlar üzərində avtomatik analizlər aparmağa imkan verir.
5. Çox faktorlu doğrulama və şifrələmə: Səhiyyə təşkilatları məlumat pozuntularını aşkar etmək və icazəsiz girişləri qarşısını almaq üçün çox faktorlu doğrulama və şifrələmə texnologiyalarından istifadə edə bilərlər. Bu, məlumatların güvənliyini artırır və potensial pozuntulara qarşı daha çətinlikli bir təcrübə tələb edir.

Bu mexanizmlər, səhiyyə təşkilatlarına məlumat pozuntularının aşkarlanması və icazəsiz fəaliyyətlərin qarşısının alınması üçün güclü bir zəmanət təmin edir. İlkin olaraq təhlükəsizlik siyasətlərinin və prosedurlarının yaradılması və tətbiqi mühüm bir addımdır. Daha sonra isə yuxarıda qeyd olunan audit və monitorinq texnologiyaları ilə sistemlər

nəzarət altında saxlanılmalı və potensial pozuntuların aşkarlanması üçün düzgün prosedurlar izlənməlidir.