قانون مسئولیت و قابل انتقال بیمه سلامت

دکتر افشین نیاکان

اطلاع رسانی پیوند داده ها

The **Health Insurance Portability and Accountability Act of 1996** (HIPAA)

قانون مسئولیت و قابل انتقال بیمه سلامت

سرفصل/ عنوان ۱: دسترسی به مراقبت های سلامت، قابلیت انتقال و تجدید پذیری در سال ۱۹۹۶توسط کنگره آمریکا مصوب شد و کلینتون نیز آن را امضا نمود

سرفصل/ عنوان ۲: پیشگیری از تقلب و سوء استفاده در مراقبت های بهداشتی ، ساده سازی اداری، بهینه سازی مسئولیت پزشکی

سرفصل/ عنوان ۳: نظارت بر مقررات مربوط به مالیات حسابهای پس انداز پزشکی

سرفصل/ عنوان ۴: جبران کاهش مالیات کارفرمایان از طریق درآمدهای حاکمیتی

سرفصل/ عنوان ۵: برنامه و اجرای نیازمندیهای گروهی بیمه سلامت

The **Health Insurance Portability and Accountability Act of 1996** (HIPAA)

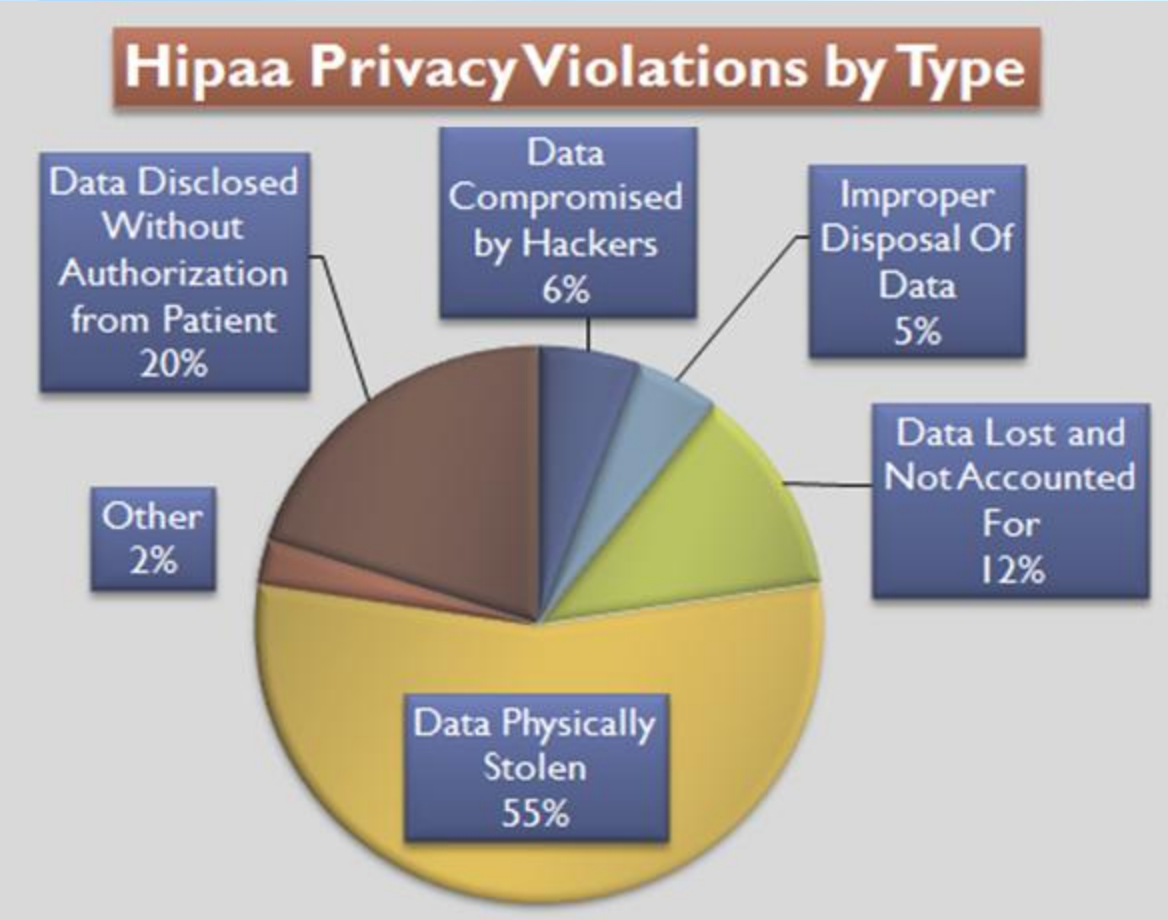
اصول سرفصل HIPAA II

1. • **Privacy Rule 2003**
2. • **Security Rule 2005**
3. • **Electronic Data Exchange**

هر قسمت توسط قانون مستقل مربوط به خود مورد حمایت قرار می گیرد

چرا سرفصل ۲ HIPAA بوجود آمد؟

ارسال گسترده ایمیل به بیماران افسرده در سال ۲۰۰۰

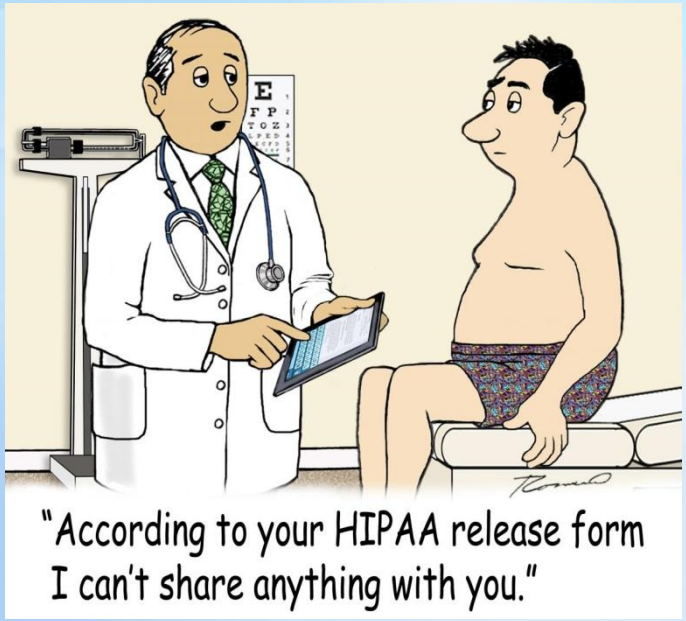


نقصهای حریم خصوصی بر حسب نوع

چرا سرفصل HIPAA ۲ بوجود آمد؟ (ادامه)

- در صورت سرقت شماره کارت بانکی، شما می تونید کارت بانکی و یا حتی بانک خود را عوض کنید.
- اما در اکثریت کشورها از جمله آمریکا نمیتونید کارت سلامت خودتان را کنسل کنید یا شناسه یکتای سلامت خود را عوض نمایید.
- پس سرقت اطلاعات هویتی بخصوص سلامت اهمیت زیادی دارد.
- با این وجود تنها بین سالهای ۲۰۰۵ الی ۲۰۰۸ ۴۰ میلیون رکورد اطلاعات پزشکی به علت رخنه اطلاعاتی تنها در آمریکا به سرقت رفته

هدف سرفصل ۲ HIPAA



- در صورت سخت گیری بیش از حد در خصوص امنیت، بخصوص موارد مربوط به حریم خصوصی و یا هنگام انتقال اطلاعات بهداشتی درمانی با اختلال جدید در عملکرد سیستم های درمانی روبرو خواهیم شد

- قوانین HIPAA برای ایجاد تعادل منطقی بین جریان آزاد اطلاعات و صیانت از حریم خصوصی بیماران وضع گردیده

ترمینولوژی های مهم HIPAA

Protected Health Information [PHI]

اطلاعات سلامت حفاظت شده

- شناسه های پزشکی (نام، آدرس، تلفن، ایمیل، شناسه پزشکی، کد ملی، عکس، تشخیص و ...)
- اطلاعات تشخیصی - درمانی هم فیزیکی و هم روانی (گذشته، حال، آینده)
- جواب آزمایش، عکس رادیولوژی، نوبت ویزیت

Treatment, Payment and Health Care Operations [TPO]

- اینها اطلاعات سلامت حفاظت شده [PHI] هستند که کادر مربوطه برای دسترسی به آنها نیازمند مجوز نیستند

Notice of Privacy Practice [NPP]

متنی که به بیمار داده می شود و اعلام میکند که به اطلاعات حریم خصوصی ذکر شده در [PHI] دسترسی پیدا میکنیم.

ترمینولوژی های مهم HIPAA (ادامه)

نهاد های تحت پوشش Covered Entities [CE]

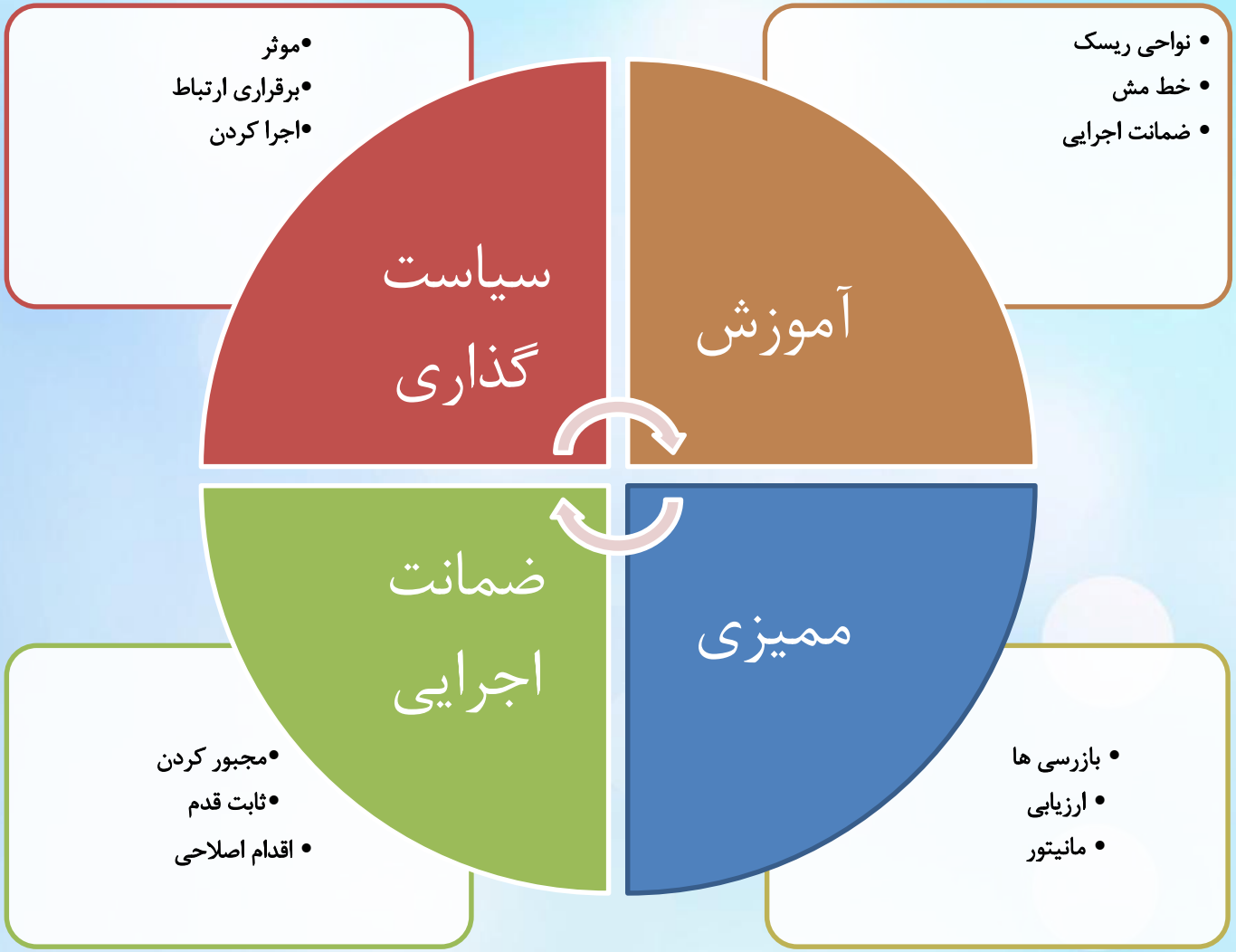
- افراد و یا نهادهایی که وظیفه رعایت قوانین و آین نامه های Hipaa را بر عهده دارند.
  - برنامه های بهداشتی – درمانی
  - کارفرمایان مراکز درمانی
  - سازمانهای بیمه یا پرداخت کننده مالی

قانون حفظ حریم خصوصی Privacy Rule

- ✓ قانون حفظ حریم خصوصی در ۱۴ آپریل ۲۰۰۳ اجرایی شد.
- ✓ حریم خصوصی اشاره به حفاظت از اطلاعات فردی مراقبت های بهداشتی دارد
- ✓ مشخص می کند که اطلاعات بیماران چگونه استفاده و افشا گردد.
- ✓ به بیماران اختیار می دهد که کنترل بیشتری بر اطلاعات سلامت خود داشته باشند.
- ✓ راه های صیانت از اطلاعات سلامت را مشخص می نماید

.

اصول پایه برنامه صیانت از حریم شخصی



Security Rule قانون امنیت

✓ آین نامه‌های امنیت (IT) در ۲۱آپریل ۲۰۰۵ اجرایی شد.

- محرمانگی اطلاعات سلامت الکترونیکی حفاظت شده ePHI
- ذخیره اطلاعات سلامت الکترونیکی حفاظت شده ePHI
- دسترسی به اطلاعات سلامت الکترونیکی حفاظت شده ePHI

قوانین امنیت و صیانت ازحریم شخصی

- توضیحات کلامی
- نوشتار
- برنامه ها و سامانه های رایانه ای
- تجهیزات و سخت افزارهای رایانه

این نکات تنها مربوط به قوانین HIPAA نیست، بلکه مربوط به انجام کار درست است.

به چه میزان آموزش برای رعایت قوانین امنیت و صیانت ازحریم شخصی مهم است؟

کجا و چگونه مجاز هستیم در خصوص بیمارانمان صحبت کنیم؟

مطابق قانون Hipaa بیمار حق دارد:

- به اطلاعات سلامت خود دسترسی داشته باشد.
- تقاضای اصلاح اطلاعات سلامت خود را داشته باشد.
- بخواهد دسترسی به اطلاعات سلامت خود را محدود نماید.
- بخواهد دیگران در مقابل افشای اطلاعات وی پاسخگو باشند.

- تمامی اطلاعاتی که در خصوص بیمار کسب می گردد محرمانه است و کسی حق افشای آنها را ندارد.
- مجازات کیفری و مدنی افرادی که از اطلاعات بیماران سوء استفاده می نمایند.
- کسی حق ندارد در خصوص اطلاعات بیماران خارج از مکان درمانی صحبت نماید.
- پزشکان و سایر کادر درمان تنها می بایست به اطلاعاتی که برای کار و یا درمان بیمار مورد نظر نیاز است دسترسی داشته باشند.
- قبل از ارائه اطلاعات بیماران به سایر افراد برای مشاوره نیاز به گرفتن اجازه از بیمار وجود دارد.
- تمامی اطلاعات کاغذی و الکترونیکی بیمار می بایست در جای امن قرار داشته باشد.
- هیچ کس حق دسترسی به اطلاعات دوستان، اعضای خانواده، کارکنان و ... را خارج از وظایف قانونی خود ندارد.
- هرگونه دسترسی به اطلاعات خارج از وظایف به اطلاعات پزشکی افراد پیگرد قانونی دارد.

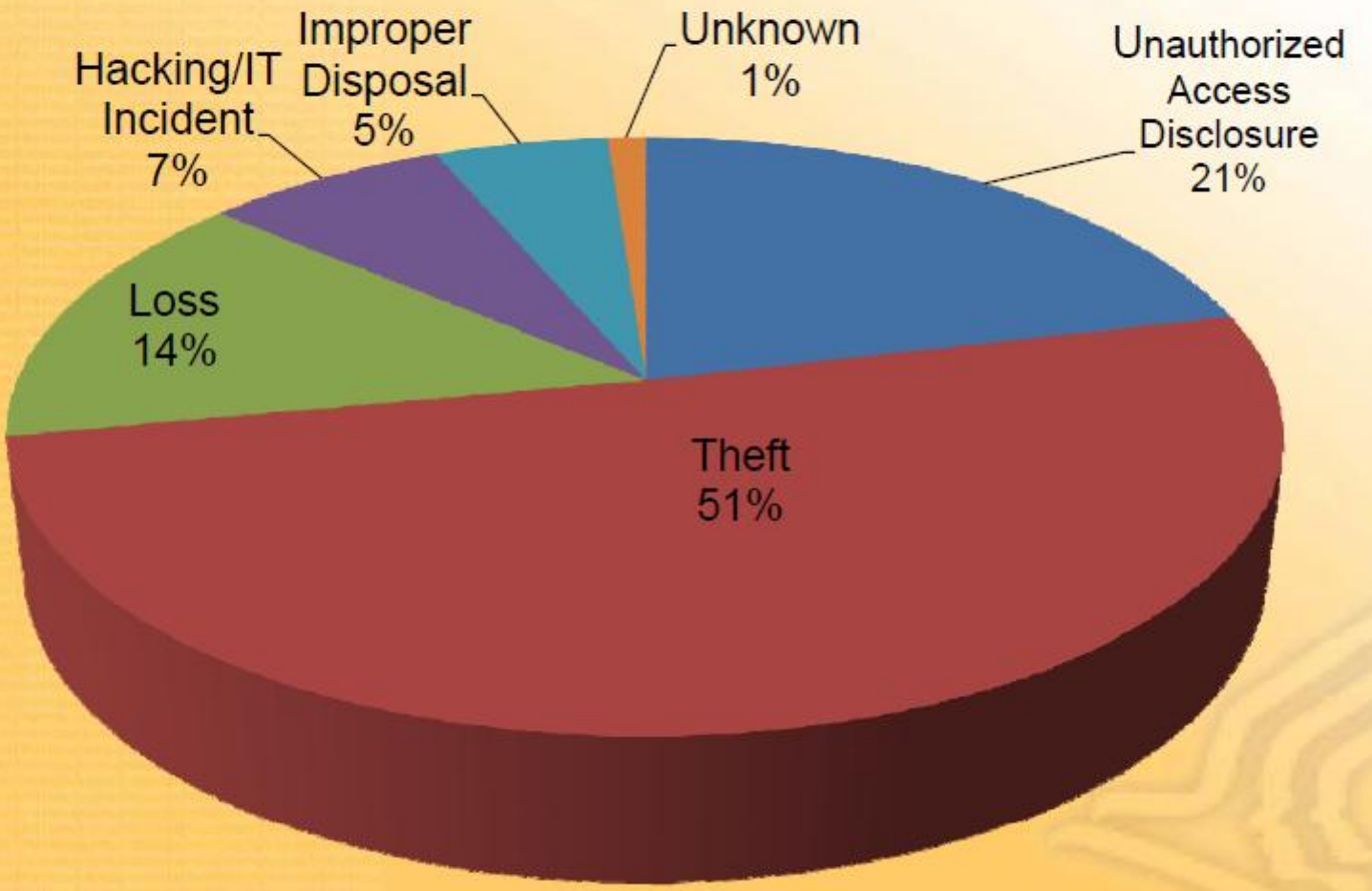
مشکلات امنیتی
در
دنیای واقعی

مطابق با گزارشات واحد خدمات بهداشتی، انسانی

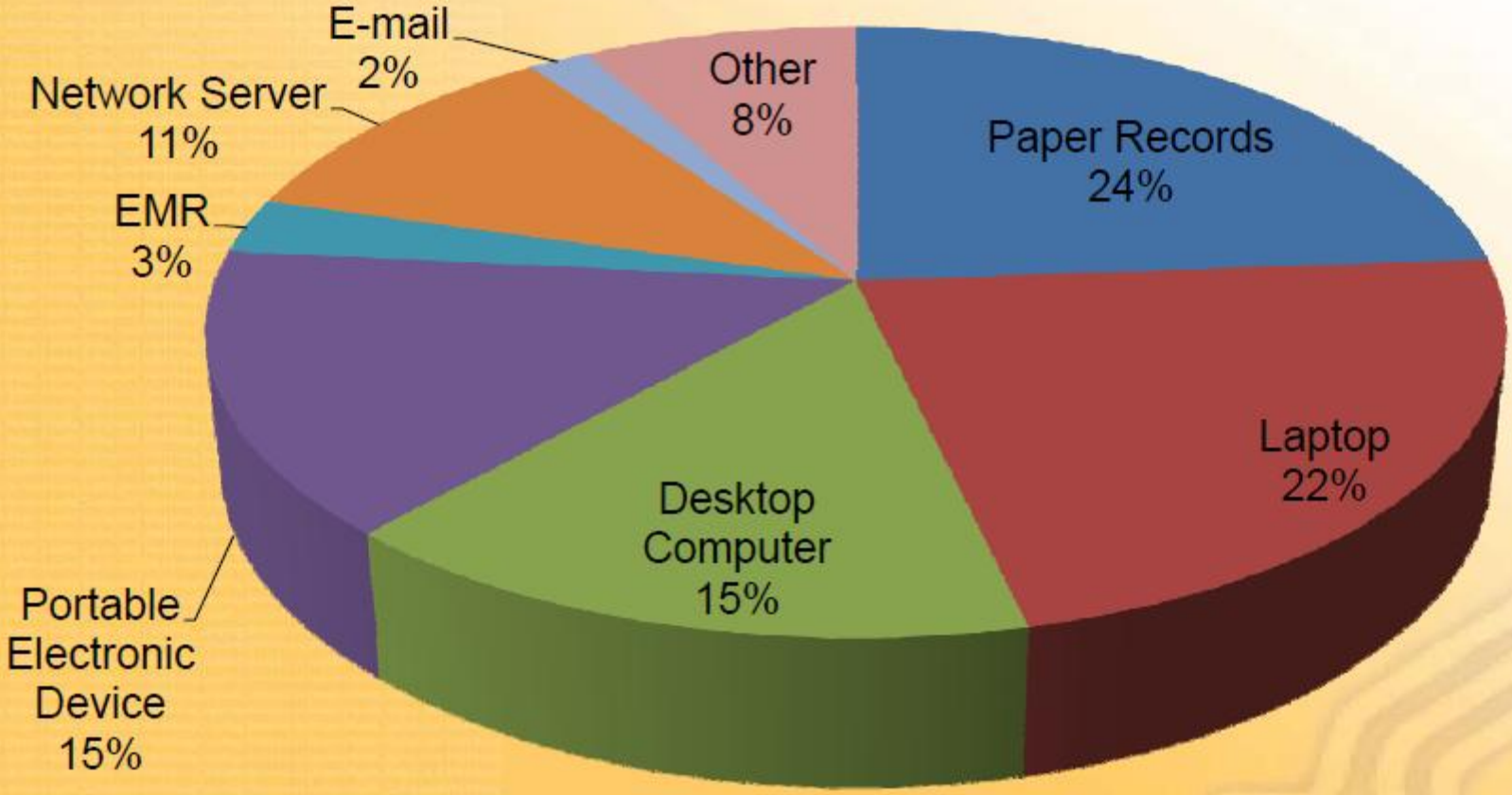
دفتر حقوق مدنی OCR (ناظر Hipaa)

Office of Civil Right

Breach Notification:
500+ Breaches by Type of Breach



Breach Notification:
500+ Breaches by Location of Breach



امنیت Hippa موارد زیر را پوشش می دهد

- حفاظت اداری
- حفاظت فیزیکی
- حفاضت فنی (امنیت سیستم و امنیت برنامه ها و داده‌ها)

حفاظت اداری:

- آنالیز و مدیریت ریسک.
- مدیریت کاربران
- آموزش و آگاهی های امنیتی
- برنامه ریزی برای پیشگیری از حوادث احتمالی
- استقرار استانداردهای مدیریت امنیت مانند ISO 27000

حفاظت فیزیکی:

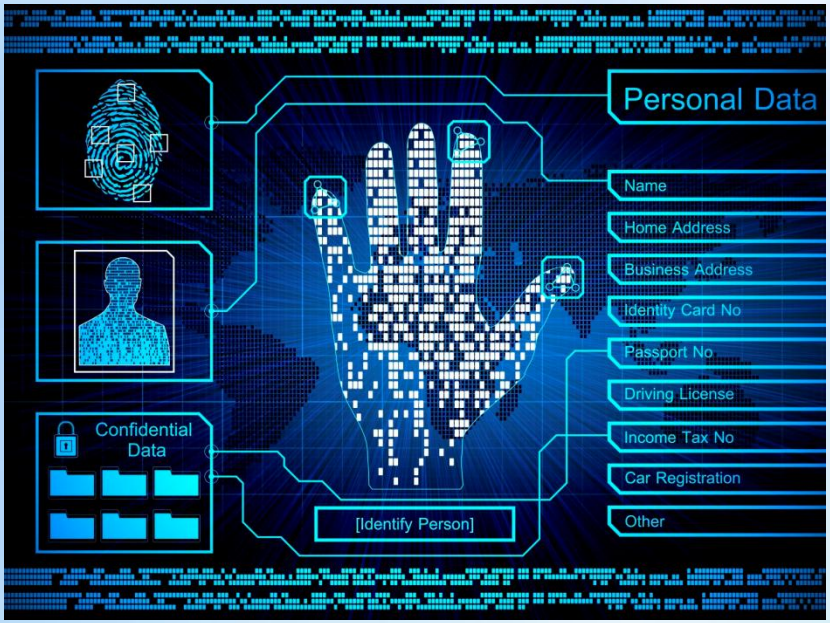
- مدیریت دسترسی به تاسیسات و اطلاعات.
- امنیت ایستگاه های کاری.
- کنترل دستگاه ها و سایر رسانه ها

حفاظت های فنی: (امنیت سیستم و امنیت برنامه ها و داده ها)

- شناسه یکتا
- رمزگذاری داده ها
- ثبت وقایع
- کنترل دسترسی اطلاعات
- احراز هویت
- اسامی رمز موثر
- احراز هویت دو عاملی در مقابل یک عاملی
- بیومتریک
- Single Sign On
- قفل شدن سیستم بعد از N بار تلاش ناموفق
- خروج خودکار از سیستم بعد از وقفه کاری

حفاظت های فنی: (امنیت سیستم و امنیت برنامه ها و داده ها) – ادامه

- قابلیت رد گیری
- نقش و حق دسترسی کاربران
- مدیریت امنیت
- (بهترین روش کنترل متمرکز با مجوز غیر متمرکز)



با تشکر:

دکتر افشین نیاکان

اطلاع رسانی پیوند داده ها