قانون قابلیت جابجایی و پاسخگویی بیمه سلامت (HIPAA)

HIPAA چیست؟

- *قاعده حفظ حریم خصوصی* HIPAA، استانداردهایی را در خصوص نحوه دسترسی، استفاده و افشای اطلاعات در WRC تعیین کرده و حقوق مراجعان را درخصوص اطلاعات مربوط به سلامتی‌شان تعریف می‌کند.

- ***قاعده امنیت*** HIPAA الزامی کرده که WRC/فروشنده برای محافظت از یکپارچگی داده‌ها و محرمانگی اطلاعات سلامتی محافظت شده، تدابیر حفاظتی فیزیکی و الکترونیکی را به اجرا آورد و حفظ کند. مثال‌های مربوطه عبارتند از: قفل کردن درها، رمزگذاری یکپارچه ایمیل و کلیدهای کارتی، خارج نکردن فایل‌های مراجع از مرکز WRC یا فروشنده.

قانون Lanterman و محرمانگی

قانون رفاه و مؤسسات – قسمت 4.5 از قانون WIC تحت عنوان خدمات برای افراد دچار ناتوانی‌های رشدی [4500 - 4885]

عنوان 17 از مقررات کالیفرنیا بخش 4514. (برای مراکز منطقه‌ای)

تمام اطلاعات و سوابق به‌دست آمده در حین ارائه خدمات پذیرش، ارزیابی و خدمات مطابق با قسمت 4.1 (که از بخش 4400 شروع می‌شود)، قسمت 4.5 (که از بخش 4500 شروع می‌شود)، قسمت 6 (که از بخش 6000 شروع می‌شود)، یا قسمت 7 (که از بخش 7100 شروع می‌شود) برای افراد دارای ناتوانی‌های رشدی باید محرمانه نگه داشته شود. اطلاعات و سوابق به‌دست آمده در حین ارائه خدمات مشابه به خدمات‌گیرندگان داوطلب یا غیرداوطلب پیش از سال 1969 نیز باید محرمانه نگه داشته شوند...

اصطلاحات - PHI

- اطلاعات جمع‌آوری شده، ایجاد شده، نگهداری یا دریافت شده که به هر صورت موجب شناسایی یک مراجع می‌گردد
- "اطلاعات سلامتی محافظت‌شده" - هرگونه اطلاعات بیمار که باعث شناسایی هویت وی شود شامل نام، آدرس، تاریخ تولد، شماره تلفن، ایمیل، فکس، SSN، شماره UCI، عکس، نام اعضای خانواده یا هر شماره یا کدی که می‌تواند به‌طور منحصربه‌فرد موجب شناسایی شخص شود
- ممکن است الکترونیکی، مکتوب یا شفاهی باشد
- شامل اطلاعات شخصی، مالی و پزشکی
- که به موارد زیر مربوط باشد:
  - شرایط جسمی یا روانی گذشته، حال یا آینده
  - سوابق درمان در گذشته، حال یا آینده

شناساگرهای فردی PHI

- نام‌ها؛
- آدرس‌ها - همه زیرمجموعه‌های جغرافیایی کوچکتر از ایالت، از جمله آدرس خیابان، شهر، کانتی، حوزه، کد پستی و کدهای جغرافیایی معادل آنها، بجز سه رقم اول کد پستی مشروط بر این که مطابق با داده‌های فعلی در دسترس عموم اداره سرشماری باشد:
- واحد جغرافیایی که با ترکیب همه کدهای پستی با همان سه رقم اول تشکیل شده و بیش از 20,000 نفر را شامل می‌شود؛ و
- سه رقم اول کد پستی برای همه این واحدهای جغرافیایی که شامل 20,000 نفر یا کمتر است و به 000 تغییر کرده است.
- تمام عناصر تاریخ‌ها (بجز سال) که مستقیماً به یک فرد مربوط می‌شود (از جمله تاریخ تولد، تاریخ پذیرش، تاریخ ترخیص، تاریخ مرگ و تمام سنین بالای 89 سال)؛
- شماره تلفن‌ها؛
- شماره فکس‌ها؛
- آدرس‌های پست الکترونیکی (ایمیل)

شناساگرهای فردی PHI

- شماره‌های تأمین اجتماعی؛
- شماره‌های پرونده پزشکی؛
- شماره ذینفعان طرح سلامت؛
- شماره حساب‌ها؛
- نام کاربری یا آدرس ایمیل حساب آنلاین، همراه با رمز عبور یا پرسش و پاسخ امنیتی؛
- شماره گواهی‌نامه/مجوز؛
- شناساگرها و شماره سریال خودروها، از جمله شماره پلاک‌ها؛
- شناساگرهای دستگاه‌ها و شماره سریال‌ها؛
- آدرس‌های وب؛
- آدرس‌های IP؛
- شناساگرهای بیومتریک مانند اثر انگشت و صدا، اسکن شبکیه و غیره؛
- تصاویر عکاسی تمام چهره و هرگونه تصویر مشابه؛ و
- هر شماره، مشخصه یا کد منحصربه‌فرد شناسایی‌کننده دیگر (به‌عنوان مثال، UCI)

مسئولیت‌های WRC/ فروشنده

- اخذ رضایت امضا شده در هر زمان که خواهان دریافت **یا** افشاء PHI نزد شخصی خارج از سازمان خود باشیم
- امکان استفاده یا افشای اطلاعات فراتر از آنچه که قرارداد یا رضایت مجاز دانسته وجود ندارد
- استفاده از تدابیر حفاظتی مناسب برای محافظت از PHI
  - تدابیر اداری - به‌عنوان مثال، تخصیص نقش‌ها/دسترسی
  - تدابیر فیزیکی - به‌عنوان مثال، قفل کردن اتاق‌ها/ کشوهای بایگانی
  - تدابیر فنی - به‌عنوان مثال، رمزگذاری الکترونیکی

مسئولیت‌های WRC/ فروشنده

- گزارش دادن هرگونه استفاده یا افشای غیرقانونی PHI به محض اطلاع از آن به DDS - به‌عنوان مثال ورود غیرقانونی یا سرقت لپ‌تاپ و ایمیل یا سایر موارد نقض امنیت داده‌ها
- حصول اطمینان از اینکه نمایندگانی که PHI را نزد آنها فاش می‌کنیم/از آنها دریافت می‌کنیم همان قوانینی را رعایت کنند که ما ملزم به رعایت آنها هستیم
- دادن اجازه دسترسی افرادی که PHI به آنها مربوط می‌شود به PHI خودشان
- دادن اجازه اصلاح کردن PHI به افراد

مسئولیت‌های WRC/ فروشنده

- دادن اجازه به افراد برای دریافت فهرست موارد افشای PHI - به همین دلیل حفظ سوابق مربوط به اخذ رضایت بسیار مهم است
- قرار دادن سوابق مربوط به PHI در اختیار دبیر بهداشت و خدمات انسانی کالیفرنیا
- برگرداندن تمام موارد PHI یا امحای آنها پس از خاتمه قرارداد
- داشتن اجازه فسخ قرارداد در صورت وقوع تخلف

جریمه‌ها

- HIPAA جریمه‌های مدنی و کیفری را برای استفاده و افشای نادرست PHI در نظر می‌گیرد
- قانون کالیفرنیا شامل جریمه‌ها و مجازات‌های بیشتری است
- HIPAA کارفرمایان را ملزم می‌کند در ازای نقض حریم خصوصی تنبیهاتی از جمله خاتمه اشتغال را اعمال کنند

جریمه‌ها

- هنگامی که شخصی آگاهانه و با نقض HIPAA اطلاعاتی را افشا می‌کند:
  - جریمه‌های مالی: حداکثر 50,000 دلار
  - حبس: حداکثر 1 سال
- هنگامی‌که به بهانه‌های دروغین انجام می‌شود:
  - جریمه‌های مالی: حداکثر 100,000 دلار
  - حبس: حداکثر 5 سال
- هنگامی که با قصد کسب منفعت صورت می‌گیرد:
  - جریمه‌های مالی: حداکثر 250,000 دلار
  - حبس: حداکثر 10 سال

چطور می‌توانم از PHI محافظت کنم؟

- هنگام کار با ارائه‌دهندگان، فروشندگان/ سایر افراد، از بهترین شیوه‌های کاری پذیرفته‌شده الگوبرداری کنید. از رمزگذاری استفاده کنید و به آنها یادآوری کنید که آنها هم از رمزگذاری استفاده کنند.
- در جامعه یا در مناطق عمومی دفتر درباره یک مراجع خاص با استفاده از نام کامل وی صحبت نکنید
- اطلاعات حاوی شناساگرهای مراجع از جمله نام، UCI یا شماره تأمین اجتماعی یا آدرس وی را دور نریزید؛ آنها را در کاغذ خردکن بریزید!
- جداول یا وسایل الکترونیکی را از دفتر خارج نکنید و آنها را در جایی قرار ندهید که کسی بتواند نام مراجع یا هرگونه اطلاعاتی را مشاهده کند

چطور می‌توانم از PHI محافظت کنم؟

- از گذاشتن پست صوتی حاوی PHI روی دستگاه پیغامگیر خودداری کنید مگر اینکه مراجع به‌طور مشخص اجازه این کار را داده باشد
- فکس یا مدارک چاپ شده حاوی PHI را در فضایی فاقد امنیت قرار ندهید
- هنگامی که مشاهده کردید PHI بدون مراقبت به حال خود رها شده است، آن را در جعبه اشیاء گم‌شده قرار دهید یا برای مأمور ناظر بر تبعیت از HIPAA ارسال کنید

چطور می‌توانم از PHI محافظت کنم؟

- اطلاعات ورود به سیستم الکترونیکی خود را در اختیار دیگران قرار ندهید و آنها را در معرض دید به حال خود رها نکنید
- هرگاه از کامپیوتر یا دستگاه الکترونیکی خود فاصله می‌گیرید به‌طور کامل از سیستم خارج شوید

کمترین حد مورد نیاز

- HIPAA الزام می کند که افشاء PHI به ***کمترین حد مورد نیاز*** برای انجام درخواست محدود شود.
- به‌عنوان مثال، اگر به پدر یا مادر کمک می کنید از WRC درخواست کند تا ارزیابی روان‌شناختی به مدرسه ارسال گردد، فقط ارزیابی روان‌شناختی ارسال خواهد شد (نه سایر سوابق پزشکی و غیره).

دسترسی به سوابق سلامتی

- مراجع یا نماینده قانونی او می‌تواند پس از ارائه درخواست کتبی، خواستار دسترسی به PHI خود به منظور بررسی و تهیه کپی از آنها شود.
- مقررات Lanterman (4725) و Early Start (303.402) همچنین به مراجعان این حق را می‌دهد که یک کپی دقیق از سوابق به‌دست آمده در جریان ارائه خدمات را بررسی، مرور و دریافت نمایند.
- ارائه‌دهنده باید به‌موقع اجازه بررسی را صادر کند، اما این مسئله به هیچ وجه نباید بیش از پنج (5) روز کاری پس از دریافت درخواست کتبی رخ دهد.
- ارائه‌دهنده باید فتوکپی‌ها را به‌موقع در دسترس قرار دهد و در هر صورت باید کپی‌ها را ظرف پانزده (15) روز تقویمی پس از دریافت درخواست کتبی ارسال نماید.

اصلاح سوابق سلامتی

- درصورتی‌که به نظر مراجعان، PHI آنها نادرست یا ناقص است، می‌توانند با ارائه درخواست کتبی، خواستار اصلاح سوابق خود شوند.
- WRC ملزم نیست با اصلاح سوابق موافقت کند، اما اگر چنین درخواستی را رد کنیم به صورت کتبی آن را اعلام خواهیم کرد
- WRC شصت (60) روز تقویمی پس از دریافت درخواست اصلاح جهت تصمیم‌گیری در مورد پذیرش یا رد آن فرصت دارد.

درخواست اعمال محدودیت

- مراجع می‌تواند از WRC درخواست کند محدودیت‌هایی درخصوص نحوه استفاده یا افشاء PHI اعمال شود.
- برای مثال، یک مراجع بزرگسال می‌تواند درخواست کند که اطلاعاتش در اختیار خواهر و برادرش قرار نگیرد.
- WRC ملزم نیست با این درخواست موافقت کند.
- WRC باید هرگونه محدودیتی را که با آن موافق است ثبت کند.

درخواست ارتباطات محرمانه

- مراجع می‌تواند درخواست کند WRC به شیوه خاصی با وی تماس بگیرد.
- WRC باید هر درخواست منطقی یا قانونی را برآورده کند.
- WRC نمی‌تواند مراجع را ملزم به توضیح دادن دلیل درخواست خود نماید.
- به‌عنوان مثال، ممکن است مراجع بخواهد که فقط در خانه با وی تماس گرفته شود نه در محل کار.

فروشندگان/ارائه‌دهندگان

- WRC با فروشندگان/ارائه‌دهندگان زیادی که خدمات مستقیمی را به مراجعان ارائه می‌دهند، همکاری می‌کند. فروشندگان/ارائه‌دهندگان نیز موظف به رعایت مقررات HIPAA هستند.

- هرگونه نقض محرمانگی که توسط فروشندگان/ارائه‌دهندگان رخ می‌دهد باید گزارش شود و توسط مأمور حفظ حریم خصوصی HIPAA مورد رسیدگی قرار گیرد. در صورت وقوع نقض مذکور، DDS الزامات گزارش‌دهی خاصی دارد

- برای اطلاع از این مقررات به مراکز خدمات Medicare & Medicaid به این آدرس مراجعه کنید: http://hhs.gov/ocr/hipaa/

رمزگذاری

- فروشندگان/ارائه‌دهندگان باید از رمزگذاری سرتاسری (EE2E) استفاده کنند که روشی برای برقراری ارتباط امن بوده و از دسترسی اشخاص ثالث به داده‌ها در حین انتقال داده‌ها از یک سیستم یا دستگاه به سیستم یا دستگاه دیگر جلوگیری می‌کند. در روش EE2E، داده‌ها در سیستم یا دستگاه فرستنده رمزگذاری می‌شوند و تنها گیرنده مورد نظر می‌تواند آنها را رمزگشایی کند.
- فروشندگان/ارائه‌دهندگان باید موافقت‌نامه همکاری تجاری (BAA) با هریک از شرکای خود داشته باشند تا امنیت PHI و انطباق کلی با مقررات HIPAA را حفظ نمایند.

خدمات رمزگذاری ایمیل منطبق با HIPAA

- Barracuda
- Egress
- Hushmail
- kIdentillect
- LUXSCI

خدمات اشتراک‌گذاری فایل منطبق با HIPPA

- Box
- Citrix ShareFile
- Microsoft OneDrive
- Google Workspace
- Kiteworks

ابزارهای توصیه شده برای رمزگذاری دیسک

- Bitlocker (ویندوز)
- FileVault (سیستم عامل mac)
- Sophos
- TrueCrypt