TOPCERTIFIER
www.topcertifier.com

วิธีการบริการ
สำหรับ HIPAA

ความสามารถในการพกพาประกันสุขภาพ
และพระราชบัญญัติความรับผิดชอบ

ข้อมูลเบื้องต้นเกี่ยวกับ HIPAA

HIPAA เป็นกฎหมายของรัฐบาลกลางที่ครอบคลุมซึ่งตราขึ้นเพื่อ:

- ปกป้องความเป็นส่วนตัวของข้อมูลส่วนบุคคลและข้อมูลสุขภาพของผู้ป่วย
- จัดให้มีการรักษาความปลอดภัยทางอิเล็กทรอนิกส์และทางกายภาพของข้อมูลส่วนบุคคลและสุขภาพ
- สร้างมาตรฐานการเข้ารหัสเพื่อทำให้การเรียกเก็บเงินและธุรกรรมอื่น ๆ ง่ายขึ้น การประกันสุขภาพ Portability and Accountability Act (HIPAA) เกี่ยวข้องกับความเป็นส่วนตัว ความปลอดภัย และการแจ้งเตือนการละเมิด กฎเกณฑ์ต่างๆ ปกป้องความเป็นส่วนตัวและความปลอดภัยของข้อมูลด้านสุขภาพและให้ข้อมูลแก่บุคคลต่างๆ สิทธิบางประการในข้อมูลสุขภาพของตน
- กฎความเป็นส่วนตัวซึ่งกำหนดมาตรฐานระดับชาติสำหรับข้อมูลด้านสุขภาพที่ได้รับการคุ้มครอง (PHI) อาจนำไปใช้และเปิดเผยได้
- กฎการรักษาความปลอดภัย ซึ่งระบุการป้องกันที่ครอบคลุมหน่วยงานและธุรกิจของพวกเขา ผู้ร่วมงานจะต้องดำเนินการเพื่อปกป้องความลับ ความสมบูรณ์ และความพร้อมของ ข้อมูลสุขภาพที่ได้รับการคุ้มครองทางอิเล็กทรอนิกส์ (phi)
- กฎการแจ้งเตือนการละเมิด ซึ่งกำหนดให้หน่วยงานที่ครอบคลุมต้องแจ้งให้บุคคลที่ได้รับผลกระทบทราบ กระทรวงสาธารณสุขและบริการมนุษย์ของสหรัฐอเมริกา (HHS); และในบางกรณีสื่อถึงการละเมิดของ PHI ที่ไม่ปลอดภัย

คิกออฟ

การประชุม Kickoff เป็นเครื่องมือสำคัญในการสื่อสารและวางแผนการดำเนินโครงการ โดยมีสิ่งกีดขวางน้อยที่สุดและเพื่อให้โครงการเสร็จสิ้นภายในเวลาและต้นทุนที่วางแผนไว้ กำหนดการ สำหรับการประชุมเริ่มต้นคือ:

- การอภิปรายแผนโครงการ: ซึ่งรวมถึงการอภิปรายเกี่ยวกับความรับผิดชอบและความรับผิดชอบของผู้มีส่วนได้ส่วนเสีย เหตุการณ์สำคัญและผลงานในโครงการ
- ขอบเขตการให้บริการ
- ข้อกำหนดทางกฎหมายและข้อบังคับ

การสร้างทีมงานหลัก

- การแต่งตั้ง CISO
- การแต่งตั้งคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ
- การแต่งตั้งเจ้าหน้าที่รักษาความปลอดภัย HIPAA

การฝึกอบรมการรับรู้ HIPAA

การฝึกอบรมการรับรู้ HIPAA จะดำเนินการให้กับพนักงานในองค์กรของคุณ ที ช่วงการฝึกอบรมเพื่อช่วยให้พนักงานได้รับความรู้ เข้าใจแนวคิด HIPAA และจัดกระบวนการและแนวปฏิบัติเพื่อให้บรรลุและจัดตั้งนำไปปฏิบัติ รักษาและปรับปรุงสภาพแวดล้อมการทำงานของระบบการจัดการบริการอย่างต่อเนื่อง เมื่อพนักงานได้รับการฝึกอบรมแล้ว พวกเขาสามารถคิดและกระทำและมีส่วนช่วยให้บรรลุเป้าหมายได้ เป้าหมาย

การดำเนินการตามระยะทีชาญฉลาด

ระยะที 1 - การวิเคราะห์ช่องว่าง

ในระหว่างระยะนี เราจะทำการวิเคราะห์ช่องว่างเพื่อตรวจสอบจำนวนแนวทางปฏิบัติในปัจจุบันของคุณ สอดคล้องกับข้อกำหนด แนวทางปฏิบัติในปัจจุบันของคุณได้รับการยืนยันโดยอิงตามข้อมูลอ้างอิงทั้งสีข้อนี เกณฑ์.

- ข้อกำหนดมาตรฐาน HIPAA
- ข้อกำหนดทางกฎหมาย ข้อบังคับ และกฎหมาย

ผลลัพธ์ของการวิเคราะห์นีนำเสนอในรูปแบบของรายงานการวิเคราะห์ช่องว่าง รายงานนี ทำหน้าทีเป็นรายการการดำเนินการเพื่อเตือนความจำของโครงการ

ระยะที 2 - ดำเนินการประเมินความเสียง HIPAA

ขั้นตอนการบริหารความเสียงจะต้องจัดทำเป็นเอกสารและใช้เป็นข้อมูลอ้างอิงในการจัดการ ความเสียงทีระบุโดยปรึกษากับหัวหน้างานของเจ้าของกระบวนการทั้งหมด เราใช้การบริหารความเสียง เทคนิคต่างๆ เช่น ISO 31000, ISO 27005,NIST,COBIT เพื่อระบุ วิเคราะห์ ประเมินผล เอกสาร จัดลำดับความสำคัญ รักษา ปริมาณความเสียงทีระบุ ขั้นตอนนีจะสร้างการลงทะเบียนความเสียง ความเสียงทีเหมาะสม แผนการรักษา ได้รับการระบุและดำเนินการตามความเสียงของบริษัท ผลลัพธ์ของการกระทำดังกล่าวจะได้รับการคำนวณ บันทึก ประเมิน และจัดทำเป็นเอกสาร การตรวจสอบความเสียงเป็นระยะ กำลังดำเนินการเพื่อให้มันใจว่าระบบปฏิบัติตามข้อกำหนด

ระยะที 3 – การพัฒนาแผนฟืนฟู HIPAA

การประเมินความเสียงหลังการทีเราช่วยเหลือในการออกแบบแผนการแก้ไข HIPAA ตามความเสียง ผลการประเมินจะกระทำโดยการประสานงานกับหัวหน้างานเป็นหลัก ดำเนินการในลักษณะทีมีประสิทธิภาพ โดยปกติแล้วแผนฟืนฟูทีเป็นไปตามมาตรฐาน HIPAA จะเป็นเช่นนัน รวม,

- สิ่งที่ต้องทำเพื่อรักษาความปลอดภัยข้อมูลส่วนตัวคนไข้ของคุณอย่างเหมาะสม
- กรอบเวลาที่สมจริงสำหรับงานเหล่านี้ที่จะต้องทำให้เสร็จ
- รายชื่อสมาชิกในทีมของคุณที่รับผิดชอบงานใด
- เอกสารประกอบการติดตามหรือเสร็จสิ้นภารกิจเหล่านี้

ระยะที่ 4 – การพัฒนาข้อตกลงสัญญาร่วมธุรกิจ

ภายใต้ HIPAA บุคคลหรือหน่วยงานภายนอกบุคลากรของคุณที่ใช้หรือมีสิทธิ์เข้าถึงข้อมูลของคุณ PHI หรือ phi ของผู้ป่วยในการให้บริการในนามของคุณเรียกว่า "ผู้ร่วมธุรกิจ" เราช่วยเหลือในการพัฒนาและทบทวนข้อตกลงสัญญาผู้ร่วมธุรกิจตาม ประเภทของผู้ขายที่ใช้บริการเฉพาะที่เกี่ยวข้องกับ HIPAA
การปฏิบัติตาม

ระยะที่ 5 – การตั้งค่ากระบวนการสำหรับเหตุการณ์การละเมิดข้อมูล

เราช่วยเหลือในการตั้งค่ากระบวนการเพื่อระบุและจัดการกับการละเมิดข้อมูล PHI (เช่น HIPAA ขั้นตอนการแจ้งเตือนการละเมิด) และยังช่วยในการพัฒนาขั้นตอนในการรายงานเหตุการณ์อีกด้วย กลไกไปยังหน่วยงานกำกับดูแลที่เกี่ยวข้อง

ระยะที่ 6 – การสนับสนุนเอกสาร HIPAA

แผนการปฏิบัติตามข้อกำหนดของ HIPAA ควรรวมนโยบายและขั้นตอนเพื่อให้มั่นใจถึงความเป็นส่วนตัวของข้อมูลสุขภาพที่ได้รับการคุ้มครองและความปลอดภัยของข้อมูลดังกล่าว นโยบายความมั่นคงและ ขั้นตอนจัดการกับ phi (PHI อิเล็กทรอนิกส์) ที่เราช่วยเหลือในการพัฒนาความเป็นส่วนตัวและความปลอดภัยของ HIPAA นโยบายและขั้นตอนสำหรับแต่ละฟังก์ชันโดยการทำความเข้าใจประเภทของ (phi) ที่พวกเขาจัดการ ด้วยความเคารพต่อ HIPAA

เจ้าหน้าที่รักษาความปลอดภัยภายในของ HIPAA การฝึกอบรมการตรวจสอบ

การฝึกอบรมผู้ตรวจสอบภายในของ HIPAA (IA) จะจัดให้กับเจ้าหน้าที่รักษาความปลอดภัยของ HIPAA การอบรมในครั้งนี้จะจัดเตรียมบุคลากรดังกล่าวเพื่อวิเคราะห์ความต้องการ IA วางแผนและกำหนดเวลา IA เตรียมการตรวจสอบการตรวจสอบ จัดทำรายการ และดำเนินการ IA และจัดทำเอกสารและรายงานข้อสังเกตต่อผู้บริหารระดับสูง

การตรวจสอบภายในของ HIPAA

ผู้เชียวชาญของเราจะดูแลการดำเนินการตรวจสอบภายในโดยเจ้าหน้าที่รักษาความปลอดภัย HIPAA ของคุณ การตรวจสอบภายในนี้จะระบุช่องว่างที่มีอยู่ในระบบและแสดงให้เห็นระดับของ ความพร้อมในการเผชิญกับการตรวจสอบการปฏิบัติตามข้อกำหนด การตรวจสอบครั้งนี้ทำให้องค์กรมีโอกาส ระบุและแก้ไขความไม่สอดคล้องทั้งหมดก่อนที่จะดำเนินการตรวจสอบการปฏิบัติตามข้อกำหนด ด้านบน ฝ่ายบริหารจะได้รับแจ้งผลการตรวจสอบภายใน

HIPAA - การวิเคราะห์สาเหตุที่แท้จริง (RCA) และการดำเนินการแก้ไข

การไม่ปฏิบัติตามข้อกำหนดทั้งหมดที่ระบุในระหว่างการตรวจสอบภายใน การตรวจสอบลูกค้าหรือบุคคลที่สาม หรือจากการลงทะเบียนความเสี่ยง, การประเมินความเสี่ยงของผู้ขาย, บันทึกเหตุการณ์, บันทึกการสำรองข้อมูล, การละเมิดข้อมูล รายงานการแจ้งเตือน จะต้องระบุแหล่งที่มาอื่นๆ RCA ดำเนินการโดยใช้เทคนิคเช่น วิธีการระดมความคิดและก้างปลา การแก้ไขและการดำเนินการแก้ไขที่เหมาะสมที่สุดคือ นำไปใช้และประสิทธิผลของการกระทำดังกล่าวได้รับการจัดทำเป็นเอกสารและตรวจสอบผ่าน HIPAA รายงานการดำเนินการแก้ไข (CAR)
ผู้เชียวชาญของเราจะอยู่กับทีมของคุณเพื่อให้คำแนะนำตลอดกระบวนการ

การตรวจสอบการจัดการ HIPAA การประชุม (MRM)

MRM เป็นโอกาสสำหรับผู้มีส่วนได้ส่วนเสียทั้งหมดที่จะประชุมตามช่วงเวลาที่กำหนดเพื่อตรวจสอบ หารือและวางแผนการดำเนินการตามวาระด้านล่าง

- ทะเบียนความเสี่ยง
- การเบี่ยงเบนในด้านการปฏิบัติตามข้อกำหนด
- รายงานกิจกรรมหลังการส่งมอบ
- แผนปฏิบัติการเพื่อแก้ไขรายการคงค้าง
- โอกาสในการปรับปรุง การเปลี่ยนแปลงที่จำเป็นในระบบ

การตรวจสอบการปฏิบัติตามข้อกำหนดของ HIPAA

เมื่อระดับความพร้อมถึงระดับที่เพียงพอแล้ว กระบวนการปฏิบัติตามการรับรองเริ่มต้นขึ้น ผู้ตรวจสอบที่ได้รับการแต่งตั้งของหน่วยงานกำกับดูแลการปฏิบัติตามกฎระเบียบ (CB) จะตรวจสอบความพร้อม ผ่านการตรวจสอบภายนอก สิ่งนี้เกี่ยวข้องกับผู้ตรวจสอบที่ต้องทบทวนนโยบาย กระบวนการ SOP และเรื่องสำคัญ บันทึกการปฏิบัติงาน และบันทึก IA และ MRM การเบี่ยงเบนที่สำคัญจากความคาดหวังของ CB จะได้รับการแจ้งให้ทราบ ณ จุดนี้เพื่อดำเนินการแก้ไขที่จำเป็น ซึ่งจะช่วยลดโอกาสที่สำคัญความไม่สอดคล้องระหว่างการตรวจสอบการรับรอง TOPCertifier จะติดต่อประสานงานกับผู้มีส่วนได้ส่วนเสียทั้งหมด และดูแลการตรวจสอบให้เสร็จสิ้น

ความต่อเนื่องของการปฏิบัติตาม

TOPCertifier จะเป็นส่วนหนึ่งของเส้นทางการปฏิบัติตามกฎระเบียบขององค์กรของคุณและช่วยเหลือคุณเป็นประจำ ช่วงเวลาที่มีการฝึกอบรมที่จำเป็น การสนับสนุนระบบและลูกสุนัข การตรวจสอบภายในและภายนอก และการต่ออายุการรับรองของคุณเป็นประจำ