ASSESSING HIPAA: HOW FEDERAL MEDICAL RECORD PRIVACY REGULATIONS CAN BE IMPROVED pdf

1: HIPAA and Compliance News - HealthITSecurity

(1) assessing hipaa: how federal medical record privacy regulations can be improved thursday, march 22, house of representatives, committee on energy and commerce, subcommittee on health.

However, the current regulation allows an exemption if the risk of harm is slight. Assessing risk can be subjective, and privacy officers have been working to create methods to conduct and document their analyses. But after a visit to his local hospital, he began to get behind on payments. The notice included the amount owed and limited information about the visit. The mistake was identified internally, and the incident was reported to the privacy officer, who had a decision to make. Did this HIPAA violation carry a significant risk of harm to the patient and thus require that he be notified of a breach to his privacy? Or-because a limited amount of information was disclosed to an immediate relative-was the risk of harm low and no notification required? For the past 11 months, privacy officers have been debating questions like this and developing processes for determining the risk of harm that comes from a HIPAA violation. However, the interim final rule included a harm threshold provision, allowing the organization to omit notification if it determined that the impermissible use or disclosure posed no significant risk of "financial, reputational, or other harm" to the individual. The provision was controversial, with consumer advocates, some providers, and even legislators claiming the threshold defied the intent of the law. Others described it as necessary, noting that it was impractical and unhelpful to notify individuals of minor errors unlikely to harm them-such as a misdirected e-mail sent within the organization or a fax mistakenly sent to the wrong clinic. Regardless of opinion, the interim rule took effect the following month, and covered entities began seeking effective processes for determining risk of harm. HHS provided some guidance on breach exemptions, but privacy officers have found that the definition of harm is unique to each case and each patient. Determining risk can be a subjective process, but organizations are identifying steps and measures that help them evaluate whether a breach notification is necessary. New Rule Increased Workload At press time, HHS had not published its final rule on breach notification, although it is expected this summer. There is a chance that the harm threshold could be removed. Regardless of the final rule, some privacy officers and HIM professionals believe risk-of-harm assessments should always be part of a HIPAA violation investigation. The last year has been a busy time for privacy and security officials. The changes led to a fresh round of privacy training within facilities, which increased the number of incidents reported to privacy officials. Davis conducts a breach investigation and risk-of-harm assessment on every HIPAA complaint or concern reported in the hospital organization. In that number jumped to 98 investigations, with 48 of those reported late in the year following the implementation of the breach notification rule. Her cases also doubled since the breach rule was instituted. Incidents Exempted from Breach Notification While HHS has not provided comprehensive guidance on determining risk of harm, it did provide the following examples of low-risk HIPAA violations in the breach notification interim final rule that are exempt from breach notification: Good faith, unintentional acquisition, access, or use of PHI by a workforce member of a covered entity or business associate Example: A staff member receives and opens an e-mail from a nurse containing protected health information about a patient that the nurse mistakenly sent to the staff person. The staffer realizes the e-mail is misdirected and deletes it. Inadvertent disclosure to another authorized person within the entity or its business associates Example: A nurse calls a doctor who provides medical information on a patient in response to the inquiry. It turns out the information was for the wrong patient. Such an event would not be considered a breach, provided the information received was not further used or disclosed in a manner not permitted by the privacy rule. Recipient could not reasonably have retained the data Example: In this case, if the nurse can reasonably conclude that the patient could not have read or otherwise retained the information, then providing the medical report to the wrong patient does not constitute a breach. Subjectivity a Challenge The way privacy officials conduct breach notification investigations and risk-of-harm assessments has been evolving since the rule was published in August Experience has led to

more refined ways to determine if a breach notification should be sent, and risk-of-harm protocol have adapted. We are handling cases differently now than before. The risk-of-harm assessment allows a privacy official to look at all the evidence and determine if that violation will cause harm to the patient and warrants a breach notification, Davis says. At Aurora Health Care, which is comprised of 14 hospitals and more than clinics, local privacy officers conduct the leg- work in investigating a HIPAA complaint. If they confirm a violation, then they forward the case to Schmidt, as chief privacy officer, for the risk-of-harm assessment. Schmidt and her privacy officers follow a documented process in assessing risk. Harm must be assessed in various categories, including the type of PHI released was there sensitive information? Using a privacy breach investigation record of some type is considered a best practice, Davis says, as it gives organizations a way to document their risk analysis decision should they be questioned on their breach notification decision either by a patient or the Office for Civil Rights, the federal organization in charge of enforcing HIPAA. A typical breach investigation record contains a brief description of the privacy complaint or concern, copies of any e-mail correspondence regarding the incident, and a series of questions that help identify the level of risk. Within the investigation record designed by Davis and used at Ministry, the risk assessment section asks questions that include: Who impermissibly used the information, or to whom was the information impermissibly disclosed? What is the potential for significant risk of financial, reputational, or other harm? What is the type and amount of PHI involved? There are some cases where determining the risk of harm is obvious, Davis says. The release of sensitive personal health information, such as diagnoses, procedures, Social Security numbers, and date of birth, should always be considered harmful and constitute a breach notification. But other incidents, like the example given at the start of this article, are less cut and dried. The information disclosed was minimal, and the mistake was a reasonable one. But what if the year-old did not want his parents to know he was being treated? What if the hospital visit centered on treatment of an STD, and the son was hiding his hospital visit from his parents? However, if the bill is for a knee injury the parents know about, the risk of harm would be minimal. Schmidt says she has learned that the individual in an unauthorized disclosure is just as significant in determining risk of harm as is the content of the disclosure. However, each investigation should follow the same process and criteria. Milwaukee-based Aurora Health Care evaluates three categories during every risk-of-harm assessment. Harm Based on Content and Recipient Both the nature of the disclosed information and the individual to whom it was disclosed influence risk of harm. A recipient of PHI who did not seek out the access, who is cooperative and willing to quickly return information, who did not have any adversarial relationship to the individual or likelihood of personally knowing the individual could be considered a "low risk recipient. Questions to consider include: What content was disclosed-just identifiers or medical, sensitive information? A bill is different than a dictation. Is it likely the recipient will be able to identify the patient whose information they received? Did the disclosure happen in a small community or a big city? What is the relationship between the recipient and the patient? Is it a family member in good standing with the patient or one half of a divorcing couple? Was the incident an intentional, unauthorized access or an accidental disclosure? Assessment of Harm by Patient Unless it is absolutely clear there is no harm, privacy officers contact the patient to discuss the incident and listen for his or her reaction as a way to assess harm. This works well for common mistakes. If a patient does not believe there is harm, privacy officers offer an apology but no further reporting to HHS is necessary. Harm Based on Assurances Received HHS states that an impermissible use or disclosure might not qualify as a breach if the covered entity obtains satisfactory assurances that the information will not be further used, disclosed, or retained. This is appropriate only in cases that are lower risk with no malicious intent. To gain this assurance: Obtain a confidentiality statement. If the recipient provides the statement and circumstances are otherwise acceptable, then no patient contact is required. Request a certificate of destruction. OCR requires that the organization must be able to demonstrate destruction. In some cases, Ministry Health Care calls patients to discuss the breach and understand how harmful the patient considers the disclosure. Before Ministry began the practice in March, Davis would err on the side of caution in borderline cases, sending a breach notification just to be safe.

But soon her staff realized that in relatively low-risk cases, the patient might be the best person to determine if risk of harm exists. Ministry only contacts patients when the risk of harm is not obvious, such as disclosures involving minimal information like patient name and the balance owed to the facility. For example, Davis has called patients when billing statements for a father have been mailed to his son who has the same name and lives at the same address. Though the risk of harm may seem low in this situation, Davis says a phone call to the father to discuss the situation can help immediately determine the risk of harm. If the patient believes that he or she has not been harmed, the case is determined to be low risk and no formal breach notification is sent to the patient or HHS. The discussion is documented in the risk assessment. If the patient cannot be reached and privacy officials are uncertain of the level of harm, Ministry sends a breach notification by default, Davis says. Davis and her team do not call individuals in cases where the risk of harm is high and a breach notification is likely warranted, such as an intentional unauthorized access or when sensitive personal information is sent to the wrong patient. The phone calls have reduced the number of breach notifications sent at Ministry, as they have at Aurora, which has a similar practice. If after reviewing all pieces of the case she remains unsure of the risk, Schmidt says she will contact the patient and discuss his or her view of the harm. In addition to assessing harm, the call also gives staff a chance to formally apologize for the breach and answer any questions the patient may have. It may be found at www. The NCHICA tool provides a way to evaluate risk of harm using a scoring system that ranks incidents from low to high risk. The tool describes the variables of a HIPAA violation-such as recipients, circumstances of release, and disposition of the information-and ranks examples of those variables from 0 to 3. The more harmful the examples in each variable, the higher their corresponding score. For example, in the "method of disclosure" variable, the incident examples read: However, it can be a useful tool, especially for those members of a risk assessment committee, such as IT or marketing, who might not have a deep background on HIPAA or the requirements of the breach rule. It helps get a consensus on what we think the risk of harm is since some of it is pre-scored before we get into the room. Even if the final rule removes the risk-of-harm assessment piece, the NCHICA tool is still a good way to document a breach investigation. The stakes for protecting patient information are much higher today, with increased HIPAA enforcement and electronic systems enabling the easy exchange of protected health information. Privacy officials should not assume certain cases are low risk without conducting a proper investigation, she warns.

ASSESSING HIPAA: HOW FEDERAL MEDICAL RECORD PRIVACY REGULATIONS CAN BE IMPROVED pdf

2: Laws and Regulations Governing the Disclosure of Health Information (update)

(iii) ASSESSING HIPAA: HOW FEDERAL MEDICAL RECORD PRIVACY REGULATIONS CAN BE IMPROVED THURSDAY, MARCH 22, House of Representatives, Committee on Energy and Commerce, Subcommittee on Health, Washington, DC.

When the HIPAA regulation initially went into effect, it generated significant skepticism, confusion, and even angst. Many in the healthcare industry asked: What did protecting the confidentiality of protected health information mean? Others worried that HIPAA would be redundant with state health privacy laws and would not add much value. People questioned whether HIPAA would really make an impact, and if any impact would be for the better or the worse. Ten years later these questions have largely been answered. Whatever one might think about HIPAA, it is hard to dispute that it has had a vast impact on patients, the healthcare industry, and many others over the last 10 years-and will continue to shape healthcare and HIM professionals for many more years to come. At the time, most medical records were in paper form, but it was becoming clear that health data would become digital in the future. The challenge of protecting privacy and security of health information was staggering in , as it can be today. Prior to , there was no federal law regulating the privacy of health information. Since the s, Congress had been passing a number of privacy statutes that protected driver license records, cable TV records, school records, and phone records. There was even a federal law regulating the privacy of video rental records-but not one regulating the privacy of health records. But because the individuals and entities that collect, use, and disclose health data are staggering in number and variety, having one regulation to rule them all would be no easy feat. Privacy was naturally a major concern with the changes contemplated in HIPAA, and it was a challenging issue, so Congress punted to the Department of Health and Human Services HHS to propose regulations to protect the privacy of health. HHS answered by proposing a privacy regulation that was finalized in These common sense standards were intended to provide a scalable, flexible framework so that all organizations across the industry-large and small, provider and health plan-could find their way toward compliance. And the balance of the [HIPAA] Privacy and Security protections have paved the way to real benefits for consumers through greater access to quality care. Enforcement has matured along with industry knowledge and capacity to meet the standards. Early on, we placed an emphasis on learning and helping covered entities weave compliance into the fabric of treatment, payment, and healthcare operations. Tools such as breach notification and audit are achieving our twin objectives of increasing public transparency and accountability of covered entities and their business associates. On the patient side, who would have thought that giving people the right of access to their health information would prove so powerful? Today, that right has become a critical component to reinventing healthcare delivery: HIPAA has improved patient access to care by delivering on a promise of privacy and security for consumers. It is my hope that the industry will continue to heed our call and adopt a culture of compliance that is essential to maintaining patient trust and public confidence. For many of us working in covered entities, shepherding our organizations toward compliance with the regulations was a major responsibility. We analyzed the regulations, forecasted likely challenges, taught the rules and their nuances to others, and strengthened our privacy and security practices. In doing so we demonstrated, once again, the value of the HIM profession. We discovered early on in our compliance efforts that change is a tall order, and that privacy and security compliance are a journey without end. But day by day, organization by organization, staff member by staff member, and process by process, we met tough challenges and improved our ability to safeguard protected health information. When we started this journey, the scope of our task seemed overwhelming. Published statistics on privacy breaches and enforcement actions are sobering. Progress was being made, but in , with the change from the Clinton administration to the Bush administration, the future of the HIPAA regulation was thrown into turmoil. The Bush administration criticized the regulations and reopened the period for comments. There were rumors that the regulation might be entirely rolled back and

restarted. The compliance deadline was set for April 14, , except for smaller health plans whose compliance date was set for a year later. HHS listened and changed it. Privacy advocates were disappointed that HIPAA allowed many uses and disclosures of information without patient consent. There was fear and confusion. We were changing the expectations of both patients and healthcare providers. A lengthy article in the October 16, , USA Today noted that thousands of providers were taking extreme measures in reaction to HIPAA-no longer leaving voicemail messages, banning office sign-in sheets, and prohibiting the sending of appointment postcards. In that same period between and there was only one HIPAA criminal action-against a lab assistant who used the personal data of a terminal cancer patient for identity theft. By , more than 33, complaints had been filed with OCR, of which about 8, were investigated. Despite the fact that about 5, investigations led to entities taking corrective action, no fines had yet been issued. HIPAA mandates that covered entities designate a privacy official to develop and implement policies for protecting privacy and handle questions and complaints. HIPAA also requires training of personnel. Limitations on Disclosure and Use. HIPAA requires that people authorize disclosure of their PHI unless an exception applies, such as a legal requirement or to report abuse, or for treatment, payment, or healthcare operations. HIPAA provides a set of rights to patients, including a right to be given a notice about the privacy practices of a covered entity, a right to access PHI, and a right to file a complaint alleging a HIPAA violation without retaliation. HIPAA did not preempt stronger state law protections, so any more protective state law remains in effect. There are also criminal penalties for certain wrongful disclosures of PHI. HIM professionals found a new career avenue as healthcare facilities developed new roles like privacy and security officers, who were hired to ensure HIPAA compliance. But just as the industry got used to the regulations, HIPAA enforcement and compliance changed in a dramatic way after This small physician group had posted appointments on a publicly available online calendar and failed to have adequate privacy and security policies and procedures, document training, or conduct a risk analysis. The high fine for a small practice group sent a powerful message that anyone could be subject to OCR enforcement. However, today many in the healthcare industry are beginning to realize the importance and seriousness of HIPAA compliance.

ASSESSING HIPAA: HOW FEDERAL MEDICAL RECORD PRIVACY REGULATIONS CAN BE IMPROVED pdf

3: HIPAA Regulations -- a New Era of Medical-Record Privacy?

Â©â€" Bioethics Research Library Box Washington DC

Patients must be assured that the health information they share with healthcare professionals will remain confidential. Without such assurance, patients may withhold critical information that could affect the quality, safety, and outcome of care. The HIPAA privacy rule became effective April 14, , and established standards for information disclosure including what constitutes a valid authorization. HIPAA applies to covered entities, defined by the rule to include health plans, healthcare clearinghouses, and healthcare providers that transmit specific information electronically. This final rulemaking provides increased protection and control of protected health information PHI. Business associates are required to comply with the same disclosure requirements as a covered entity, and these expectations typically will be addressed in the business associate agreement between the covered entity and the business associate. This practice brief provides a general overview of the laws and regulations impacting the timely and appropriate release of PHI. The act strengthened privacy and security requirements and broadened patient rights to accessing and restricting the uses and disclosures of PHI. Preempts state law contrary to the privacy rule except when one of the following conditions is met: This does not include past unrelated medical problems. These disclosures are permitted and not required. This can now be considered a breach based on the outcome of the breach risk assessment Requiring the update to the notice of privacy practices for all organizations to include the requirements as updated under the Omnibus Rule Prohibiting the use of genetic information by health plans for underwriting purposes Finalizing breach notification requirements: It grants people the following rights: The act also applies to record systems operated pursuant to a contract with a federal government agency. The Patriot Act is primarily a vehicle for the US government to enhance its ability to monitor and detect activities that may indicate the support for terrorism. The act is not necessarily targeted at protected health information PHI or systems that create, store, or manage such information. Nonetheless, it is conceivable that in pursuit of investigations being conducted under this act, a demand for PHI may be made of any healthcare provider who would be expected to comply AND who would be prevented from informing the subject of the investigation that is, the patient. Confidentiality of Alcohol and Drug Abuse Patient Records This rule 42 CFR, part 2 establishes additional privacy provisions for records of the identity, diagnosis, prognosis, or treatment of patients maintained in connection with a federally assisted drug or alcohol abuse program. When these regulations are less stringent than those of the final privacy rule, the final privacy rule would prevail. In general, the rule: In the final rule, health information includes genetic information. Health plans and insurers are prohibited from imposing a preexisting condition exclusion based solely on genetic information and from discriminating in individual eligibility, benefits, or premiums based on any health factor, including genetic information. Written procedures govern use and removal of records and include conditions for release of information. Information from or copies of records may be released only to authorized individuals, and the hospital must ensure that unauthorized individuals cannot gain access to or alter patient records. Original medical records must be released by the hospital only in accordance with federal or state laws, court orders, or subpoenas. Written procedures govern use and removal of records and the conditions for release of information. State Laws and Regulations State laws relative to the privacy and confidentiality of patient health information vary widely. States may have special privacy requirements for patients tested, diagnosed, or treated for alcohol and drug abuse, sexually transmitted diseases, or mental health disorders. There may also be privacy and confidentiality requirements within state legislation or regulation related to insurance, workers compensation, public health, or research. The best practice is to always follow the more restrictive regulatory guidelines when releasing information. Accreditation Standards In standard IM. The hospital has a written policy addressing the privacy of health information. The hospital implements its policy on the privacy of health information. The hospital uses health information only for purposes permitted by law and regulation or

as further limited by its policy on privacy. The hospital discloses health information only as authorized by the patient or as otherwise consistent with law and regulation. The hospital monitors compliance with its policy on the privacy of health information. Standards of Practice Except where a consent or authorization clearly indicates otherwise, disclosures of information made pursuant to a valid authorization will be for information originated on or before the authorization was signed. Except as otherwise required by federal or state law or regulation, or specified in the authorization itself, the date an authorization expires is ultimately left up to the policy of the individual organization. Recommended expiration date for authorizations is no more than one year from date the authorization was signed by the appropriate party. Recommendations To ensure compliance with federal and state laws and regulations that protect the confidentiality of health information and govern its disclosure, HIM professionals should: Identify policies, procedures, and processes that must be developed or revised to comply with these standards. Become knowledgeable about other applicable federal laws and regulations relative to privacy, confidentiality, and disclosure of patient health information. Become knowledgeable about state laws and regulations relative to privacy, confidentiality, and disclosure of health information. To this end, links to state laws and regulations provided on state health information management association Web sites may prove helpful. Consider performing a key word search of state laws by accessing AllLaw. Develop an understanding about which rule prevails or how various requirements can be combined procedurally. For example, how can a health information manager combine the requirements for the notice of information practices in the privacy rule with those in the Confidentiality of Alcohol and Drug Abuse Patient Records rule and any requirements in state law? As another example, consider the necessary modifications to the release of information fee schedule to comply with both federal and state regulations insofar as reasonable charges. Establish policies and procedures that comply with federal and state laws and regulations. Ask legal counsel to ensure that new and revised policies and procedures comply with all federal and state laws and regulations. Train members of the work force on policies and procedures with respect to protected health information. Maintain appropriate documentation to demonstrate compliance with federal and state privacy laws and regulations. Review contracts with any business associates to whom information is disclosed and make sure the language contained therein is in compliance with the state and federal laws. Monitor compliance and implement corrective action where indicated. Non-covered entities that maintain individually identifiable health information are encouraged to construct policies and procedures in which information obtained or disclosed is the minimum necessary, the work force is trained about the importance of privacy and confidentiality, and consumers are:

4: Do HIPAA Regulations Need Updates on Patient Privacy?

Assessing HIPAA: how federal medical record privacy regulations can be improved: hearing before the Subcommittee on Health of the Committee on Energy and Commerce, One Hundred Seventh Congress, first session, March 22,

5: Assessing Hipaa: How Federal Medical Record Privacy Regulations Can Be Improved

The BiblioGov Project is an effort to expand awareness of the public documents and records of the U.S. Government via print publications. In broadening the public understanding of government and its work, an enlightened democracy can grow and prosper.

6: HIPAA Turns Analyzing the Past, Present and Future Impact

Assessing HIPAA: how federal medical record privacy regulations can be improved Paperback - January 9, by United States Congress (Author), United States House of Representatives (Author), Committee on Energy and Commerce (Author) & 0 more.

ASSESSING HIPAA: HOW FEDERAL MEDICAL RECORD PRIVACY REGULATIONS CAN BE IMPROVED pdf

7: No Harm Done? Assessing Risk of Harm under the Federal Breach Notification Rule

1. File Cours Pratique De Construction Navale Part 3 Professe Lecole Superieure De Maistrance De La Marine French Edition 2. Read Ocr As A Level Law Book 1.

ASSESSING HIPAA: HOW FEDERAL MEDICAL RECORD PRIVACY REGULATIONS CAN BE IMPROVED pdf

Discovering Whales Dolphins Ibc code 2012 V. 1. Lake states V. 24. Lower Canada and Iroquois, 1642-1643 Automatic car parking system project using arduino Geographic visualization concepts tools and applications Pictorial history of Paisley Women as leaders in education Alcohol advertising does not target children Jacob Sullum Ill tell you in person Engine 2 diet meal plan On the Eighth Day The history and antiquities of dissenting churches and meeting houses, in London, Westminster, and Southw Asset management configuration in sap A Nation of Steel Behold the sign of salvation, a noosed rope : the promise and perils of Du Boiss economies of sacrifice Biological effects of radiation on human body Mann, T. Introduction to Demian. 2016 it skills and salary report Full Woman, Fleshly Apple, Hot Moon The Ascent Of Mount Carmel The bro code full version Tlc Talking and Listening With Care The philosophy of common law Content analysis by Kristina M. Spurgin Barbara M. Wildemuth Policymaking for school library media programs Faeries Landing, Vol. 5 Ready-to-use Celtic designs. Your first day of serious videoing Dr. Prestons Daughter November/Pentecost/Ordinary time Inbreeding, Incest, And The Incest Taboo Stigma notes on the management of spoiled identity Two . in the field Calamity at Apache Wells From Rochester to Andersonville Bowkers Complete Video Directory 1998 (Bowkers Complete Video Directory 4 Vol Set) Midas touch trump kiyosaki Hyundai sonata repair manual Sharks and troubled waters