



February 12, 2019

Secretary Alex M. Azar II
U.S. Department of Health and Human Services
Office of Civil Rights
Attention: RFI, RIN 0945-AA00
Hubert H. Humphrey Building
Room 509F
200 Independence Avenue SW
Washington, D.C. 20201

RE: "Request for Information on Modifying HIPAA Rules to Improve Coordinated Care" (RIN 945—AA00)

Dear Secretary Azar,

Thank you for requesting information from the public on modifying HIPAA prior to issuing a Notice of Proposed Rulemaking (NPRM). We support the right of patients to keep their private medical information confidential, thus we have long opposed HIPAA due to its intrusion on the patient-doctor relationship and its infringement of privacy rights. Our opposition continues today and has only grown with the EHR mandate, MIPS/APMs, HIEs, eHealth Exchange, and interoperability mandates.

As we often say, "He who holds the data makes the rules." Thus, protecting patient privacy protects not only the confidentiality of private information, but the individual freedom and choices of citizens. Our organization, Citizens' Council for Health Freedom (CCHF), has been engaged in a two-decade campaign to inform Americans that despite what they've long been told by the news media, government agencies, health plans, legislators, Congress, hospitals, and doctor's offices:

- HIPAA is not a privacy rule.
- HIPAA gives outsiders legal license to share, use, analyze, link, and sell patient data.
- HIPAA empowers corporations, government, health plans and others to profit from access to and use of confidential patient information without the patient's consent.

Therefore, we appreciate this opportunity to share our concerns about HIPAA for your consideration before publication of the NPRM. The following are general comments on privacy, HIPAA, and the value-based health care purpose of the OCR RFI, followed by answers to several specific questions.

General Comments:

Patient Privacy:

HIPAA is a broadly *permissive* data-sharing rule for use of data (internal sharing) and for disclosure of data (external sharing). Consequently, we are concerned about this phrasing in the RFI: "The Privacy and Security Rules limit the circumstances under which covered entities may use and

disclose PHI [protected health information] and require covered entities to implement safeguards to protect the privacy and security of PHI.”

Many Americans will read “limit the circumstances” and think this means *limited circumstances*. However, there are relatively few circumstances in which patient data cannot be shared, used, disclosed, compiled, analyzed, dissected, and if stripped of 18 identifiers, sold or given away. These uses and disclosures are *permitted without patient consent* under the broad definitions of payment, treatment and “health care operations,” as well as the deidentification standard, the 12 national priority purposes, the treatment exemption to the “minimum necessary” requirement, and more.

That HIPAA leaves patients powerless over the disclosure and use of their data was underscored by **David Brailer**, the first National Coordinator of Health IT:

“You can’t force a covered entity to give your data to someone you choose, and you can’t stop them from giving it to someone they choose.” (*Healthcare IT News*, May 1, 2015)

Or as ONC has previously stated:

“It’s a common misconception that [HIPAA] makes it difficult, if not impossible, to move electronic health data when and where it is needed for patient care and health.” (The Real HIPAA, *Health IT Buzz*, n.d.)

Sharing is determined by covered entities, which “may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.” (Summary of the HIPAA Privacy Rule, July 26, 2013)

HIPAA “improves the flow of health information.” (The Real HIPAA, *Health IT Buzz*, n.d.)

Value-Based Payment and Transformation

OCR issued this RFI to seek “*public input on ways to modify the HIPAA Rules to remove regulatory obstacles and decrease regulatory burdens in order to facilitate efficient care coordination and/or case management and to promote the transformation to value-based health care...*”

First, we are concerned because these three terms are broad, vague, and subjective. For example, one person’s “case management” is another person’s restrictive treatment protocol. One person’s “care coordination” is other person’s method for keeping patients from having a physician oversee their care. One person’s “value-based health care” is another person’s power to withhold physician payment or patient care.

We believe the federal push to expand data sharing under these three terms, which in today’s vernacular have come to mean third-party interference in medical decision-making, and third-party profiteering at the expense of the patient, will further impose central control over the practice of medicine and disrupt—or altogether end—patient-centered care.

Second, value-based payment will create a conflict of interest between patients and doctors.

We believe that the costs and bureaucratic burdens of the EHR mandate, and the imposition of the data-focused Merit-Based Incentive Payment System (MIPS) Alternative Payment Models (APMs), and Value-Based contracts have led more physicians to shut down their private practices and become employees. This has focused their attention on the demands of their employers for intrusive data reporting and compliance with the corporation's restrictive treatment protocols, rather than on their professional obligation to address the patient's individual needs for care, comfort and cure.

Third, we believe “value-based payment” is being used to virtually *outlaw* the free-market, fee-for-service payment system—and thus reduce access to physician care. Imagine telling one's attorney or plumber that they'll be paid or not paid according to one's own definition of “value” after the fact. There would be fewer and fewer attorneys and plumbers. Likewise, we expect fewer physicians to remain in practice and fewer applicants of excellence at medical school. Already, experienced doctors are retiring early, many of them burned out from the mandated EHR and the ever-growing, multi-layered bureaucratic requirements imposed by government, hospitals and health plans. Increasingly, patients have practitioners without medical training (non-physicians) as their only ready source of care. In a 2016 survey by The Physicians Foundation, 48% of 17,200 doctors were looking to fully or partially exit hands-on patient care, despite 10,000 baby boomers entering Medicare every day, many headed into the most medically-complex time of their lives.

Fourth, value-based payment controls may lead to lower-skilled doctors. Physicians will not be allowed to charge for the hours they work or the expertise and special skills that they have, and may be denied payment altogether for certain services or certain patients. In fact, many may choose not to develop their skills or further their education since there is no expected return on the investment—an extreme loss for patient care, innovation and medical excellence. Furthermore, VBP will exert control over their medical decisions despite the 1965 Medicare law, which prohibits such control:

“Nothing in this title shall be construed to authorize any federal officer or employee to exercise any supervision or control over the practice of medicine, or the manner in which medical services are provided, or over the selection, tenure, or compensation of any officer, or employee, or any institution, agency or person providing health care services...” (§1801)

Fifth, “value” is also a highly subjective term. From *Morning Consult*, Feb 6, 2019:

“In a Jan. 30 interview, [U.S. Senator James] Lankford acknowledged the difficulty of arriving at a consensus on the definition of value-based payment. . . . The Oklahoma senator noted that these are ‘relative, subjective decisions.’”

“[I]t's very hard to agree on the data you're measuring for the outcomes...It goes back to what providers have told us: There are so many externalities. Did they [the patient] take the drug; did they take it correctly; are there other lifestyle factors that should be involved.?” - Ben Isgur, PwC, PwC survey

Sixth, government is rarely, if ever, an engine of positive transformation. The government is an engine of regulation and police power, often “transforming” an industry away from freedom, and the

choices and lower prices of a true and fully-functioning free-market. That has indeed been the effect of Medicare. Value-based payment, imposed by government in collaboration with health plans, will not be transformative. It will be destructive of medical excellence and individualized patient care.

Seventh, outsiders will be in control of the data, dollars and decisions at a time when the patient is most vulnerable. These corporations or government agencies will be empowered to use the data, massage the data, and report the data as they see fit, perhaps claiming “lack of value” even if the subsequent payment decision:

- harms the patient
- partially or fully modifies the physician’s behavior in a way that harms broad swaths of patients over time (standardized care mandated for non-standardized patients), or
- impedes access to care that meets the patient’s needs and the patient’s definition of value

Bottom Line: OCR should not strengthen outsider controls by legitimizing the terms of “care coordination,” “case management,” and “value-based health care,” which can be interpreted however powerful players, including government, choose to interpret them. Embracing these terms will lead to officially-sanctioned violations of the patient-doctor relationship, professional obligations, and medical ethics. Instead of expanding data sharing in clear violation of the patient’s rights to confidentiality and non-interference in the exam room, we encourage OCR to move toward patient ownership and personal control over confidential patient information. OCR should also use its authority to advance patient-doctor decision-making within the professional obligations and clinical expertise of physicians and other practitioners, and within the context of what’s best for the patient.

OCR Authority to Act on Behalf of Patients:

As a reminder, U.S. Code §1320d-2 only requires the Secretary to “adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically.” Nothing requires HHS to eliminate patient consent to enable patient data to be exchanged electronically. Nor does patient consent preclude electronic data exchange.

When the HIPAA rule was first finalized by the Clinton administration, it *included patient consent* requirements for data-sharing related to treatment, payment, and health care operations. More than 50,000 comments had been filed in response to the NPRM, a majority of them requesting consent requirements. But industry later asked the new Bush administration to re-open the rule and strike the consent requirements, which the Bush administration did. It also established a “Limited Data Set” (LDS) allowing patient data to be shared without patient consent for “research,” “public health,” and “health care operations” (a nearly 400-word list of activities) under a data-use agreement. While it acknowledged that patients could be re-identified in the LDS, it said the DUA would prohibit it.

Specific RFI Questions – CCHF Response

Clearinghouses (QUESTION 5) – Clearinghouses should stay solely under BA requirements, and not be allowed to disclose and use data permissively as a covered entity. Today, clearinghouses can only process nonstandard health information data into standard data elements solely for claims

processing and only under business associate data-use agreements that limit the use of the data. Given that clearinghouses have data on 90% of all health care claims transactions, changing the rule to give clearinghouses the same right to share patient data without patient consent as other covered entities -- the entities that actually care for or pay the expenses of most patients -- would give the clearinghouse a priceless pot of gold, comprehensive patient data to share with/sell to the highest bidders, and leave patients even more unaware of data-sharing under HIPAA than they are today. Most patients probably have no idea that clearinghouses exist.

As **Adrian Gropper MD** writes in *The Health Care Blog* (3/24/17): “By giving the infrastructure business the right to use and sell our data without consent or even transparent, we are enabling a true panopticon—an inescapable surveillance system for our most valuable personal data.” Quoted in *Politico Morning eHealth* (12/22/17), he says, “Privatizing involuntary surveillance via clearinghouses is even worse than having the government do it. At least the government would be subject to some public interest constraints.”

Disclosure Requirements (QUESTION 7 - lines 1-9) - No, and no. *Treatment Example:* Doctor A could request information from Doctor B that the patient doesn’t want Doctor A to have. The patient should have the right to refuse to disclose treatment information. Consent should be required. *Payment and Health Care Operations:* Under HIPAA, with its broad permissiveness, Hospital A could claim they need the patient’s data from Hospital B for payment purposes despite the data having nothing to do with the condition for which the patient is in Hospital A. Likewise, the vast list of health care operations have virtually nothing to do with clinical care, and written, informed, voluntary patient consent should be a requirement.

Non-HIPAA Entity (QUESTION 9) - Counterintuitively for those who think HIPAA protects privacy, it is perhaps safer for patient privacy and data security to send data to a non-HIPAA entity, which is not under the permissive HIPAA rule that allows the data to be broadly shared and used. The non-HIPAA entity may thus be more constrained in their use and sharing of the individual’s data. But consent should still be required.

Psychotherapy Notes and Genetic Information (QUESTION 11) - All patient information should have the same privacy protections as psychotherapy notes, sexually-transmitted diseases, genetic information and other so-called “culturally-sensitive” information. Individuals have their own definitions of sensitive and reasons for refusing to share certain data. Consent should be required.

Right to Opt Out (QUESTION 13) - Individuals should have the right to restrict disclosures of their information through consent. Consent (opt-in) should be the standard, not opt out. Opt-out is dissent, not consent, and it gives outsiders the first right of access, use, and ownership—until the data subjects figure out what’s happening, learn they can stop it, figure out how to stop it, and take action to stop it. The burden in opt-out is on the patient, who has less time, money, and access to the facts.

42 CFR Part 2 and State Laws (QUESTION 14) - *Every* individual should have the right of consent that those protected by 42 CFR Part 2 have today. And in conformity with HIPAA (the law) and the privacy and consent interests of patients, and for the protection of patients, state laws that are stronger and more protective should continue to supersede HIPAA’s permissive data-sharing rule.

Explicit Affirmative Consent (QUESTION 15) - Yes, before initiating a request to share PHI, the covered entity should get explicit affirmative written consent from the patient. The entity's "professional judgement"—a subjective standard potentially infused with conflicts of interest—should not be the standard. Patient consent—written in black and white—should be the standard.

Information Blocking (QUESTION 16) - Let *patients* block all information they choose to block. It's their confidential information, and their lives, quality of life, choices, and reputations that are at stake.

Minimum Necessary Requirement (QUESTION 17) - There should be no exceptions, and that includes data-sharing for treatment, which under the current minimum-necessary standard does not disallow the sharing of a patient's entire medical record to whomever is treating them today. Furthermore, "population health" focuses on tracking and analyzing patients without their consent. And review for appropriateness of care and utilization, as well as formulary development, may use confidential patient data to limit the patient's access to treatment, according to the views, budgets, and agendas of health plans, government agencies and other corporate and self-interested outsiders.

Public Outreach on HIPAA (Question 20) - Outreach to share the truth about HIPAA is vitally important. However, in our experience, when people learn the truth about HIPAA, they are shocked. For two decades they have been told and led to believe that HIPAA protects their privacy. Therefore, unless they are allowed to limit the data that is used and shared, even for needed housing and access to social services, these individuals may not be agreeable to such sharing. On the other hand, it's important to realize that these individuals may not feel the freedom to say no to such sharing even if they want to due to fear of losing services—or they may choose in the future, after learning the truth about HIPAA, to protect themselves (e.g. not being truthful in the doctor's office).

Opioids and Serious Mental Illness (Question 22-24) - The exam room is supposed to be a sanctuary of safety, but HIPAA's permissive sharing, the EHR mandate enabled by HIPAA, and state Prescription Monitoring Programs (PMPs) make the exam room an unsafe place of data collection, government surveillance, and unwanted exposure. For example, when Prince died, the Minnesota PMP was accessed without authorization. At least two Minnesota and three Indiana pharmacists were disciplined, but more may have accessed his information without consequence.

Parents, Children, and Spouses (Question 25) - CCHF has heard complaints from parents who have no idea what treatments have been prescribed for their children and are therefore unable to protect and advise them. We've heard of clinics that tell parents to leave the room of a pre-teen or teenage child so private conversations can happen with, and be recorded by, a stranger to the child -- a stranger with an agenda that may not be in the child's or family's best interest. We've also heard from parents who are paying the bills for coverage of care they're not allowed to know or inquire about. And we've heard from spouses who are denied access to information about how their spouse is being treated. One physician told CCHF he wasn't allowed to see his spouse's medical record in the hospital in which he worked, and he didn't learn until almost too late that a key medication was not being given. The staff wouldn't answer his questions, making him feel helpless to protect his wife as she decompensated.

“Accounting of Disclosures” Requests (Question 27) - We believe patient requests for AoD are rare. Since patients believe HIPAA protects their privacy, why would they request an accounting of disclosures? Several years ago, we asked staff in more than 20 congressional offices what signing the HIPAA form meant and almost to a person they said it meant their information was just between them and their doctor.

Business Associate Disclosures (Question 31) – Yes, every disclosure to a business associate (BA) and by a BA should be accounted for and reportable to the patient. No, patients should not have to contact BAs for the information. There is no patient-business associate relationship. Every click on the Internet can be tracked and recorded; the doctor’s every treatment decision and every nurse’s use of the EHR is recorded and tracked. Thus, it is possible to track every disclosure through an EHR. Every request for a disclosure and every access for a use can also be tracked and recorded.

The Health Insurance Portability and Accountability Act of 1996, combined with the HIPAA “Privacy” Rule and the 2009 EHR mandate, has facilitated unmitigated, ongoing access to patient data for a multitude of purposes, including non-clinical uses and disclosures to which a patient has not consented, by all sorts of individuals and corporations that the patient knows nothing about (there are >700,000 covered entities and 1.5 million business associates per HHS in 2010).

Eric Schmidt, technical advisor and former chairman of Alphabet Inc, Google’s parent company had tried to do a project with health care data in the past but failed. At HIMSS 2018, he said:

“The arrival of the EHRs is a major story in the last decade because ten years ago they didn’t exist in the form that we know today. We forget that they didn’t exist. And before that it was impossible to get the health care data.” (March 5 keynote address, HIMSS 2018 video)

Don Rucker, MD, National Coordinator at ONC, at the same conference talked about how smartphones and apps could potentially add to the profiling and analysis of individuals:

“Either you’re looking at things that don’t have medical data, or you’re looking at things that just have medical data. You’re not looking at things that synthesize knowledge about our environment and our lives and our behaviors with medical data. That is really the opportunity here.” (*Healthcare IT News, March 7, 2018*)

Carl Dvorak, president of Epic, the nation’s largest EHR system, told *Healthcare IT News* in 2015:

“When I think of population health, I think of algorithms. . . . We need a support system for the algorithmic workers and the caseworkers to sift, sort, slice, dice, and understand their population...”

Claims that tracking and reporting disclosures to patients is too expensive or difficult ignore what’s already happening in the EHR (ongoing tracking, use, and sharing of patient data). **If those sharing and receiving patient data don’t wish to keep the subject of the data in the loop about these specific activities, the simple solution is to stop disclosing and using the patient’s data.**

Another possible solution: According to Grand View Research, “The market for storing and analyzing health information is worth **more than \$7 billion a year**” (*The Wall Street Journal*, 11/27/2018). If there are in fact additional costs for accounting for these disclosures and making them available to the subjects of the data, charges for disclosures and uses of the patient’s data could cover them. In addition, OCR could require that patients receive payments for the use and disclosure of their data. For each disclosure and transaction unrelated to the immediate and current clinical care of the patient, patients could receive a *Data Use and Disclosure* report and an associated payment. Today, patients have no idea about these disclosures and uses, have no power to stop them, and have received no financial benefit from their own data while others reap billions in benefits without their consent. This type of “pay-the-patient” mandate would enable transparency, impose accountability, likely provide a sense of fairness to the data subjects, and potentially curb data-sharing excesses and objectionable uses.

Under HIPAA, the many corporations patients know about (e.g. hospitals, health systems, health plans) and many corporations they don’t know about (other covered entities and 1.5 million business associates) are profiting off patients through uses and disclosures of patient data without patient consent. At the very least, patients should know the full extent of this data transfer and the extent that it’s being used for wealth generation—and they should be given the opportunity to profit from their own data or end the use and sharing of it.

Notice of Privacy Practices and Accounting of Disclosures (Question 35, 36, and 38) – No, the NPP is insufficient to inform about the accounting of disclosures, starting with its name, which is deceptive at best. HIPAA and the NPP name shout “patient privacy” but whisper “no patient consent for sharing and using your confidential data.” Why would a patient worry or ask about an accounting of disclosures when they think that their data cannot be disclosed without their consent?

Data Elements in Accounting of TPO disclosures (Question 37 and 40) – Patients have a right to know what’s actually happening to the confidential data in their medical records, who disclosed their data, who received their data, who the recipient shared it with, who is using their data, how much their data was sold for, how much was charged for retrieval and submission of it, for what purposes, the legal authority under which it was disclosed or used, and for how long. Yes, names of recipients and specific purposes (not just “treatment” or “research” or “health care operations” etc.) should be disclosed to patients. The information could be shared via the online patient portal, as well as in other ways (email, paper, fax) for patients who don’t want to join or use the portal.

Accounting for non-EHR Disclosures (Question 41) – Yes, patients have a right to know how their confidential data is shared and used without their consent regardless of if an EHR is used. The right to know is not limited by the format of the data or the method of data-sharing.

NPP Signing as Condition of Receiving Care (QUESTION 45) – For more than five years, Citizens’ Council for Health Freedom has encouraged patients not to sign the so-called HIPAA “privacy” form or the acknowledgement statement regarding the NPP. No law requires patients to sign it, but doing so has thoroughly propagated the myth that HIPAA protects the confidentiality of patient medical records. This misinformation has left patients vulnerable, unengaged and complacent as their confidential data is shared and used widely without their consent, including uses

that interfere with their access to care and impose penalties on their doctors for treating them according to their individual needs rather than a standardized treatment protocol embedded in and tracked by the EHR.

CCHF also has a reporting form on our website (**HIPAAhurtme.com**), where we have gathered and continue to gather stories from patients who've had to fight to not sign the form, given in and signed the form because they needed care and couldn't wait, or were refused treatment and left the office.

Bundled Consent Forms (Question 47) – CCHF has actively opposed the coercive use of consolidated (bundled) consent forms to secure the patient's signature when the patient would otherwise refuse. Patients are vulnerable by their very nature – they cannot secure what they need for care or cure on their own—yet practices and institutions on whom they depend hand them consent forms that include “consent for treatment” at the top of the form and all sorts of other consents below and then demand a single signature of agreement when they're least able to refuse.

For example, the **North Memorial Clinic consent form has 9 items** and the following statement before the signature line:

“By signing below, I consent to all of the above and I acknowledge that I have received a copy of the North Memorial Notice of Privacy Practices.”

As another example, **Essentia Health has 22 items**, with the 22nd item being the NPP:

“V. If this is my first visit to this Essentia Health location, I acknowledge that a copy of the current Notice of Privacy Practices has been provided to me and is available to me via postings in the registration areas and on the website....”

The two-page Essentia Health form also says,

“I understand that Essentia Health will treat me whether or not I consent to sections L-M and O-S of this document.”

This appears to mean that if the patient refuses to consent to the provisions of A-K, N, and T-V (**V is the NPP acknowledgement**), the patient will not be treated.

See screenshots of both organization's forms below.

NORTH MEMORIAL CONSENT FORM

(<https://www.cchfreedom.org/files/files/North%20Memorial%20Consent%20Form.pdf>):



Patient: _____

MRN: _____

DOB: _____

Consent for Services

A. Consent for Treatment. I consent to the physicians, referral physicians or their assistants, and designees of North Memorial to examine, treat, complete tests, complete routine procedures and to administer such medications considered necessary or advisable.

B. Blood / Exposure Testing: I understand that if a health care worker is accidentally exposed to my blood or other body fluid my blood will be tested for the presence of bloodborne pathogens (hepatitis B, hepatitis C, and human immunodeficiency virus) in accordance with public health policy in order to protect and counsel the exposed individual. The results of such tests will be part of my medical record and will not be released except as required or permitted by law.

Screening for human immunodeficiency virus may be done if determined by a physician to be appropriate in accordance with public health policy.

C. Release of Medical Records. I agree that information from my medical record may be used by or given to physicians, referring providers, staff, and/or business associates as necessary for treatment and healthcare operations, so long as any release of information is in compliance with the law.

D. Release of Medical Records for Medical or Scientific Research. Medical records, regardless of when generated, may be released for the purpose of medical or scientific research unless a written objection is completed. This release may be revoked by me in writing at any time.

E. Disclosure of Presence. I understand that during my visit my friends, family, or others, may call to inquire about my presence at North Memorial. I authorize North Memorial to disclose information about my presence and/or location at this facility to anyone who may inquire about me by name. This may, when appropriate, include a one-word description of my condition: critical, serious, fair or good.

F. Personal Property. I understand North Memorial is not responsible for the loss of any valuables.

G. Payment and Insurance Consent. I request that payment be made to North Memorial on my behalf for any services furnished me by North Memorial, including physician services. I authorize any holder of medical or other information about me to release to any insurance company/payor responsible for payment, any information needed to secure payment. I agree to pay North Memorial for all charges not covered by any third party. I agree to the release of information to any payor or external vendor chosen by a payor to meet authorized utilization review and quality reporting requirements

H. I have received a copy of the North Memorial Notice of Privacy Practices.

I. Consent to Disclose Information. The following consent is on behalf of third party payors. I authorize my insurance company or health plan administrator to share my records with North Memorial about services that I have received from hospitals, clinics, physicians, and other care providers that are unrelated to North Memorial. My insurance company or health plan administrator may share my North Memorial records with a health care provider system or accountable care organization in which North Memorial participates. These records allow my insurance company or health plan administrator to share information within the care provider system or accountable care organization to better coordinate my care and to improve the quality of the care I receive.

By signing below, I consent to all of the above and I acknowledge that I have received a copy of the North Memorial Notice of Privacy Practices.

Date _____ Time _____
 Verbal/Telephone consent obtained by: _____

Signature of Patient or Patient's Representative

(If Patient's Representative, under what legal authority are you signing?)

Witnessed by: _____

Reason patient unable to sign: _____

Parent Guardian Health Care Agent
 Other (specify): _____

Follow-Up:

Date: _____ Initials: _____ Note: _____

ESSENTIA HEALTH CONSENT FORM (page 2; <http://mnbright.com/pdf/Meridian.pdf> and <https://www.cchfreedom.org/files/files/Essentia%20Health%20Meridian%20consent%20form.pdf>):

parties who are responsible for, or who facilitate, payment of my bill, fraud investigation, care management, or quality improvement. This includes behavioral health and chemical dependency information. Essentia Health may also release my protected health information to suppliers of medical equipment, special transportation, or other health services so they can request payment from my insurance or other payer. I also authorize Essentia Health to release my protected health information to organ procurement organizations to facilitate donations, and to e-Prescribing networks to facilitate prescription management.

N. I authorize Essentia Health to release information from my medical records: as needed by the Federal Food and Drug Administration (FDA) or manufacturers of drugs or medical devices to contact me about defects or recalls; or to emergency service providers involved in my care before and during transport to Essentia Health, for quality improvement.

O. I authorize Essentia Health to release information from my medical records and source data as needed to accrediting organizations and to legally authorized agencies to oversee healthcare activities and to physician specialty boards for board certification/re-certification of physicians.

P. I authorize Essentia Health to release information from my medical and billing records for scientific and health services research to improve patient care and delivery. I may object at any time to release of my protected health information for scientific research.

Q. I authorize my bill to be combined into one statement that covers all members of my household. Results of tests and treatments will not be included on the bill. I authorize Essentia Health to discuss bill or payment issues with an adult household member who gives my name, address, date of birth, and either my account number or insurance ID number as well as his or her own name and address.

R. I authorize Essentia Health to disclose my presence and religious preference to Essentia Health Chaplains and to clergy of my denomination, and to disclose my presence to foundations that support Essentia Health and its mission. I understand that Essentia Health will ask specific permission before disclosing my presence for behavioral health or chemical dependency services.

S. I agree to the presence of students, observers from other healthcare facilities, healthcare consultants and approved representatives of medical service providers during tests, exams, medical treatments and other services at Essentia Health. I understand that Essentia Health will also seek my oral permission to have non-Essentia Health persons present during any services.

T. I authorize my health insurance plan to release to Essentia Health my protected health information about services I have received from Essentia Health and other care providers unrelated to Essentia Health. Essentia Health may use this information for treatment, payment, operations and case management purposes.

U. I understand that this authorization ends one (1) year from the date signed except for purposes of payment and research.

V. If this is my first visit to this Essentia Health location, I acknowledge that a copy of the current **Notice of Privacy Practices** has been provided to me and is available to me via postings in the registration areas and on the website www.essentiahealth.org. I understand that I can ask for a copy of the notice at any time.

- o I understand that I may revoke this permission at any time by notifying Essentia Health in writing. No further release will take place after the date notified.
- o I understand that other parties may use or disclose health information received from Essentia Health.
- o I understand that Essentia Health will treat me whether or not I consent to sections L-M and O-S of this document.
- o I understand I will receive a copy of this form.
- o For care provided in Wisconsin: I understand Wisconsin law gives me the right to inspect and receive a copy of behavioral health and chemical dependency information to be disclosed.


If I am signing as Authorized Representative of the patient, I am:

Parent of a minor Court appointed guardian/conservator Other: _____
(Please specify relationship to patient)

Signature (Patient or Authorized Representative) Date Time

Witness (signature by mark must be witnessed)

Patient Name & Medical Record Number
OR
Patient Label

 **GENERAL CONSENT AND AUTHORIZATION**
Page 2 of 2

Electronic Signatures (QUESTION 47) – Some patients report being asked to sign an electronic pad that is blank except for a signature line. The staff tells them that they are signing the HIPAA

acknowledgement form, or in other cases, that they are signing a consent form, but they do not know what they are signing. Some have refused to sign, and requested a paper form instead. Some patients have had to fight to get a copy of this paper form to read. Others have been told to still sign the electronic form after they read the paper form. Some have refused because they still do not know what they are actually signing. Others have only agreed to sign the paper form, despite how unhappy the clinic administrative staff were with their refusal to sign the electronic pad.

Removing NPP “Good Faith” Requirement (QUESTION 51) - CCHF is not opposed to removing the requirement, but wants the public to be fully informed about what HIPAA actually is and what it allows. For nearly 20 years, the American public has been told that HIPAA is a protective privacy rule while their data has been shared with countless outsiders for countless purposes, many of them likely objectionable to these patients, without their consent. Today, with EHRs, HIEs, eHealth Exchange, Epic’s Care Everywhere, and other clinical data registries that often pull all their data together into a singular view of the patient, two unrelated doctors or hospitals, or a patient’s physical therapist or X-ray technician, may be able to see all their diagnoses, including STDs, depression, cancer, or the use of a practitioner that the patient chose not to disclose.

HIPAA’s primary focus is not privacy; it is *security* of the data before, after and while patient’s privacy is being violated, which is what happens when the patient’s data is disclosed and used without the patient’s consent. If privacy were the focus, the HHS “Wall of Shame” would be littered with documentation of all the times patient privacy is violated every day. HIPAA does not protect the patient data the way patients think it does or in the way patients define and interpret the word “privacy.” Instead of requiring patients to sign a statement that wrongly convinces them that their data is held in confidence, OCR should have practitioners and institutions make a good faith effort to have patients sign a form/statement that faithfully and ethically shares the truth about HIPAA. Thus, in response to this specific question, we suggest OCR modify the:

- Name of the *PRIVACY RULE*. Instead of “*Standards for Privacy of Individually Identifiable Health Information* (“Privacy Rule”),” as noted on the HHS HIPAA website (<https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>), change the name to “*Standards for Disclosing and Using Patient Data Without Patient Consent.*”
- Name of the *NOTICE*. Change “Notice of Privacy Practices” to “Notice of Permitted Data Disclosures Without Patient Consent” (NPDD) and require actual definitions (full text) of “treatment” “payment,” “health care operations” and a list of the 12 national priority purposes (45 C.F.R. §164.512) to be included within the notice.
- Text of the *ACKNOWLEDGEMENT STATEMENT*. Change it to say, “I understand that the federal HIPAA regulation permits sharing and use of my personally-identifiable health information without my consent, including to the government and various corporations for non-clinical and other purposes. I further acknowledge that I have received a copy of the *Notice of Permitted Data Disclosures Without Patient Consent* and I have reviewed the federal purposes and definitions that permit data sharing without my consent—unless a stronger state medical privacy law exists to prevent such uses and disclosures. Finally, I acknowledge that I have reviewed my right to request restrictions on data sharing and that

my provider must provide me with a form to do so at my request, but that my provider is allowed to agree or refuse to agree to my request for restricted sharing of my information and must inform me of such agreement or refusal, or future changes in such an agreement.

- Process for REQUESTING RESTRICTIONS on data sharing. OCR should produce a standardized form that every practitioner and institution must make available upon request.

OCR should also require the new Notice (NPDD) to **include the more restrictive requirements of state law**, as the Mayo Clinic Notice of Privacy Practices includes today, but few others do. OCR should also engage in an **information campaign** on this requirement as well as the right of state legislatures to pass stronger, more protective state laws that require informed written patient consent. Unfortunately, most state legislators, like congressional staffers, also incorrectly believe HIPAA is a privacy-protecting rule rather than the permissive data-disclosing rule it is.

MAYO NOTICE WITH STATE LAWS INCLUDED:

<https://www.mayoclinic.org/documents/becomingpat-rst-privacypractices-rst-pdf/doc-20079394>

At the very least, OCR should:

- Prohibit doctors and hospitals from telling patients that HIPAA is a privacy rule, or that it protects their privacy.
- Require doctors and hospitals to tell patients that HIPAA is a data-disclosure rule permitting disclosures of personally-identifiable patient information without patient consent,
- If OCR continues to require practitioners and institutions make a good faith effort to get a signature acknowledging receipt/understanding/reading of the NPP, prohibit them from refusing to treat patients if patients refuse to sign the acknowledgement.
- Require notification of patients on how the patient can easily access a full accounting of all disclosures and uses of their private medical data.

***NOTE:** these suggestions for QUESTION 51 are unnecessary if OCR restores the patient's pre-HIPAA privacy and consent rights.*

Aware of HIPAA Rights (Question 53) – Yes, individuals are not fully aware of their HIPAA rights, but much more disturbing is the fact that their rights do not include the right to keep their private medical records confidential, leaving every patient vulnerable and insecure to the peering eyes and assessments of outsiders, and leaving patients and their doctors subject to the dictates of those that hold the patient's data and make the rules for how or if patients receive the care that they want and need (predictive analytics, standardized treatment protocols, payment withholds, "quality" measures, pay-for-performance metrics, "value"-based payments, etc.)

We conclude with these SIX requests for OCR action in a Notice of Proposed Rulemaking to Modify HIPAA:

- 1) Restore the patient privacy and consent rights that were in place pre-HIPAA.

- 2) Initiate and enforce a “Truth about HIPAA” campaign for the American people, including their state legislators and members of Congress.
- 3) Acknowledge and support that patients have a right to keep their confidential information truly confidential. It’s up to patients to decide whether to agree to share their confidential data in particular if the benefits, including third-party payment for care, give them sufficient reason to share the data for that purpose, but perhaps only for that purpose, and limited to the data necessary for that purpose alone.
- 4) Write the NPRM from the understanding that interoperability is not and should not be the end goal; the goal should be the protection of the patient’s rights, privacy, confidence, security, safety, access to care, and trust. After all, the point of the entire health care system is the patient and the integrity of the system rests on how the patient is treated and cared for.
- 5) Write the NPRM from the understanding that the lack of full, unmitigated, 24/7 interoperability today is the only thing that protects patients *from* HIPAA and its permissive use and sharing of their confidential data without their express consent (unless a stronger, more protective state law exists).
- 6) Write the NPRM from the understanding that patient consent requirements do not inhibit interoperability. They just limit disclosures and uses to those that the *subject of the data* (the patient) permits – as it should be.

Thank you for this opportunity to respond to your questions regarding potential modifications to HIPAA in advance of issuing an NPRM. Please do not hesitate to contact the CCHF office with questions, or for any additional information.

Sincerely,



Twila Brase, RN, PHN
President and Co-founder