GW | GARFUNKEL WILD, P.C. ATTORNEYS AT LAW

LONG ISLAND HEALTH INFORMATION MANAGEMENT ASSOCIATION
An Overview of the Proposed Changes to the HIPAA Privacy Rules

April 21, 2021

Presented by:

Robert A. Del Giorno, Esq.
Partner / Director
rdelgiorno@garfunkelwild.com

Kathleen M. Brown, Esq.
Associate
kbrown@garfunkelwild.com

Great Neck, NY 516.393.2200 | Hackensack, NJ 201.883.1030 | Stamford, CT 203.316.0483 | Albany, NY 518.242.7582

www.garfunkelwild.com

BACKGROUND

- On January 21, 2021, the DHHS Office of Civil Rights (OCR) published a Notice of Proposed Rule Making.
  - **Purpose** = propose amendments to provisions in the HIPAA Privacy Rule that OCR believes could present **barriers to coordinated care and case management** or impose other regulatory burdens on healthcare providers and individuals.

See 86 Federal Register 6446, available at
https://www.regulations.gov/document/HHS-OCR-2021-0006-0001

- In formulating the proposed rules, OCR considered over 1300 public comments it had received following publication of its December 18, 2019 "Request for Information on Modifying HIPAA rules to Improve Coordinated Care" (RFI).
  - The RFI followed the 2018 launch of the DHHS' "Regulatory Sprint to Coordinated Care."

BACKGROUND

- The January 21, 2021 Proposed Rule Making originally had a public comment period ending on March 22, 2021, but the cutoff date has since been extended to **May 6, 2021**.
  - 889 public comments have been posted (as of 4/2/2021).
  - OCR is again seeking comment on specific questions that it has posed for each proposed revision.

- The **effective date** of any final rule based on the proposed rules would be 60 days after publication in the Federal Register.
  - Covered entities and business associates would be expected to be in compliance with the final rule no later than 180 days from the effective date.
  - OCR would begin enforcement of any new or revised standards 240 days after publication of a final rule.

NEW DEFINITION PROPOSED: ELECTRONIC HEALTH RECORD (EHR)

- *Electronic health record* means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and their staff.
  - Clinicians include, but are not limited to, health care providers that have **direct treatment relationships** with individuals, such as physicians, nurses, pharmacists, and other allied health professionals.
    - "Health-related information on an individual" covers the same scope of information as the term "individually identifiable health information."

ELECTRONIC HEALTH RECORD (EHR)

- Not applicable to "indirect treatment relationships" *i.e.*, providers who deliver health care based on orders of another health care provider and typically provide services, products or reports to another care provider.
  - For example, a DME provider that supplies equipment to other providers, who then supply the equipment to individual patients.

NEW DEFINITION PROPOSED: PERSONAL HEALTH APPLICATION

- *Personal health application* means an electronic application used by an individual to access health information about that individual, which can be drawn from multiple sources, provided that such information is managed, shared, and controlled by or primarily for the individual, and not by or primarily for a covered entity or another party such as the application developer.
  - This contemplates services offered directly to consumers to monitor their own health status. It does not include, for example, patient portals.

PROPOSED REVISED DEFINITION: HEALTH CARE OPERATIONS

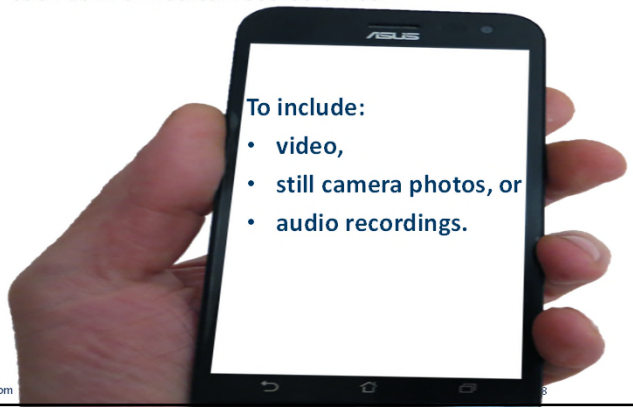
- *Health care operations* includes conducting quality assessment and improvement activities, that include:
  - outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities;
  - patient safety activities (as defined in 42 CFR 3.20);
  - population-based activities relating to improving health or reducing health care costs;
  - protocol development;
  - case management and care coordination;
  - contacting of health care providers and patients with information about treatment alternatives; and
  - Related functions that do not include treatment.

Currently, this is a comma

- ***OCR hopes the insertion of a semi-colon will clarify that each activity listed after are separate types of health care operations whether population-based or individually focused.***

RIGHT OF ACCESS

- OCR would modify provisions regulating individuals' right of access to PHI by:
  - Strengthening individuals' rights to inspect their PHI in person, which would include allowing individuals to ***take notes or use other personal resources to view and capture images of their PHI*** after arranging a "mutually convenient time and place" for the individual to inspect their PHI in a designated record set, such as in a medical records office.



"Mutually convenient time and place" includes at the point of care., e.g., viewing x-rays at a health care appointment.

RIGHT OF ACCESS – *NOTES/OTHER PERSONAL RESOURCES TO VIEW AND CAPTURE IMAGES OF PHI*

- Covered entities:
  - would not be required to allow an individual to connect a personal device (*e.g.*, a thumb drive) to the covered entity's information systems and
  - may impose requirements to ensure that an individual records only PHI to which the individual has a right of access.
    - Reasonable policies and safeguards could be established to ensure, for example, that an individual's use of personal resources minimizes disruptions to the covered entity's operations, and is used in a way that enables the individual to copy or otherwise memorialize only the PHI in the individual's designated record set to which the individual is entitled.
    - Covered entities would not be permitted to establish policies and safeguards that impose unjustified or unreasonable barriers to individual access.

RIGHT OF ACCESS – OBSTACLES AND DELAYS

- Complaints regarding access:
  - inconsistent or incomplete uploading of electronic records to health information exchanges;
  - entities that routinely respond to access requests on day 29 with a demand for additional clarifying information in writing in order to process the requests; and
  - entities that only respond when threatened with legal action.

RIGHT OF ACCESS – OBSTACLES AND DELAYS

- Harmful effects on health when the process to access records is too complicated or when the provision of records is delayed or denied:
  - need to repeat tests and procedures because medical history information was not available;
  - delayed referrals and inaccurate diagnoses based on incomplete information; and
  - lack of timely information needed for self-care.

RIGHT OF ACCESS – *FORM AND FORMAT*

- The covered entity may require an individual to make a request for access in writing (in electronic or paper form).
  - Must inform individuals of this requirement (current regulation).
- **Proposal:** Covered Entities may not impose **unreasonable measures** that impede the individual from obtaining access when a measure that is less burdensome for the individual is practicable for the entity.

A "reasonable measure" could include (for example) :

  - requiring individuals to complete a standard form containing only the information the covered entity needs to process the request.

RIGHT OF ACCESS – *FORM AND FORMAT*

Unreasonable measures include (for example) requiring an individual to do any of the following:

- fill out a request form with extensive information that is not necessary to fulfill the request;
- obtain notarization of the individual's signature on a request form; or
- submit a written request only in paper form, only in person at the entity's facility, or only through the covered entity's online portal.

RIGHT OF ACCESS – *FORM AND FORMAT*

- OCR clarifies that "readily producible" copies of PHI include copies of ePHI requested through secure, standards-based application programming interfaces (APIs) using applications chosen by individuals, and that they also include copies in any form and format required by applicable state and other laws.
  - OCR example: if a covered entity or its EHR developer BA has chosen to implement a secure, standards-based API* that is capable of providing access to ePHI in the form and format used by an individual's personal health application, that ePHI is considered to be readily producible in that form and format, and that is also the manner by which the ePHI is transmitted.

In other words, where ePHI is readily producible in the electronic form and format requested by the individual, the covered health care provider must provide that access, including when the individual requests access to the ePHI through a secure, standards-based API via the individual's personal health application.

* must be consistent with ONC's Cures Act certification criteria and the covered entity's Security Rule obligation.

RIGHT OF ACCESS – *NEW STANDARD PROPOSED FOR DIRECTING E-PHI TO THIRD PARTIES*

- **Background:**
  - **Current regulation** – 45 CFR 164.524(c)(3)(ii) – Directs covered entities to transmit a copy of PHI directly to another person designated by the individual, upon the individual's written, signed request.
  - In January 2020, a Federal District Court ruled that this regulation impermissibly exceeded the HITECH Act which had only granted a limited right to individuals to direct a copy of ePHI in an EHR to a third party in an electronic format.
  - Further, the court ruled that DHHS impermissibly broadened the application of the access fee limitation (the "patient rate") to apply to copies of PHI directed to third parties, as DHHS failed to subject this requirement to the normal notice and comment rulemaking process.
  - The Court vacated the regulation.

Ciox Health, LLC v. Azar, et al., 435 F.Supp.3d 30 (D.C. Dist. Ct. 2020)

RIGHT OF ACCESS – *NEW STANDARD PROPOSED FOR DIRECTING E-PHI TO THIRD PARTIES*

- Consistent with the court's opinion, which the government did not appeal, OCR now seeks public comment on proposals to:
  1. narrow the scope of the access right to direct records to a third party to **only electronic copies of PHI in an EHR**; and
  2. apply new fee limitations to the access right to direct a copy of PHI to a third party, as described below.

RIGHT OF ACCESS – *NEW STANDARD PROPOSED FOR DIRECTING E-PHI TO THIRD PARTIES*

- **Proposed Rule**: Individuals would be able to direct a covered entity to transmit an **electronic copy** of PHI in an EHR directly to another person (third party) that the individual designates.
  - Such access must be provided when the individual's request, made orally or in writing (including electronically), is ***clear, conspicuous, and specific***.

For example:

- an oral request that identifies the designated recipient and where to send the PHI could meet this standard.
- Additionally, this provision would allow an individual to use an internet-based method,* such as a personal health application, to submit an access request to their health care provider to direct an electronic copy of their PHI in an EHR to a third party, so long as it is "clear, conspicuous, and specific."

*e.g., patient portals, mobile "apps" and successor technologies

RIGHT OF ACCESS – *NEW STANDARD PROPOSED FOR DIRECTING E-PHI TO THIRD PARTIES*

- The **proposal** would also extend the right to direct copies of PHI to a third party by adding an express right to request that covered health care providers and health plans submit an access request to covered health care providers for electronic copies of PHI in an EHR on behalf of the individual.
  - If an individual is a current or prospective new patient of a covered health care provider, or an enrolled member or dependent of a health plan, and the individual makes a clear, conspicuous, and specific request that their health care provider or health plan submit an access request for electronic copies of PHI in an EHR to another covered health care provider, the first health care provider or health plan ("Requester-Recipient") would be required to submit the request on behalf of the individual as soon as practicable, but no later than 15 calendar days after receiving the individual's direction and any information needed to make the access request.
  - The requirement would be limited to requests to send the electronic PHI back to the covered entity that submitted the request on behalf of the individual.

RIGHT OF ACCESS – *NEW STANDARD PROPOSED FOR DIRECTING E-PHI TO THIRD PARTIES*

- A covered health care provider that receives an individual's access request ("Discloser") for an electronic copy of PHI maintained in an EHR by or on behalf of the Discloser, from a health care provider or health plan Requester-Recipient that is clear, conspicuous, and specific,
  - (*e.g.*, clearly identifies the Requester-Recipient, the scope of the requested PHI and where to transmit it)
- would be required to transmit the requested electronic copy to the Requester-Recipient, consistent with obligations under the access right to direct a copy of PHI to a third party.

RIGHT OF ACCESS – *RESPONSE TIME*

- Covered entities' required response time to requests by individuals to exercise their right of access would be shortened to "as soon as practicable," but in no case later than 15 *calendar* days (from the current 30 days) with the opportunity for an extension of no more than 15 calendar days (from the current 30-day extension).
  - Only one 15 calendar day extension would be permitted
- Where another federal or state law requires a covered entity to provide an individual with access to the PHI requested in less than 15 calendar days, that shorter time period will be *deemed practicable* under the Privacy Rule.
  - OCR notes that at least 8 states currently require health care providers to provide copies of PHI within 10 -15 days.

RIGHT OF ACCESS – *RESPONSE TIME*

- A covered entity may discuss aspects of the individual's access request with the individual before fulfilling the request, but such clarification of the request would not extend the time limit for providing access.
  - This should help address situations described in public comments in which covered entities contact individuals for the first time near the end of the initial compliance deadline to discuss the request or obtain additional information, and then take unnecessary additional time beyond that initial deadline to fulfill the request.
- The same timeliness requirements would be applied when an individual requests direct access and when an individual requests that an electronic copy of PHI in an EHR be directed to a third party.

RIGHT OF ACCESS – *RESPONSE TIME*

- OCR would also require covered entities to establish written policies for prioritizing urgent or other high priority access requests (especially those related to health and safety) so as to limit the need to use 15 calendar-day extensions for such requests.

➡ Examples of urgent or high priority requests:

- when an individual voluntarily reveals that the PHI is needed in preparation for urgent medical treatment, or
- the individual needs documentation of a diagnosis of severe asthma to be allowed to bring medication to school.

RIGHT OF ACCESS – *FEES*

- **Concern**: Ensuring that covered entities *do not profit* from disclosures of PHI made at the individual's request.
- The **Proposed rule** revises the ability to charge a fee for the cost of *supplies* by limiting such fee to the cost of supplies *for creating a non-electronic copy*.
- Fees may still be charged for the cost of labor for:
  - copying the PHI (whether in non-electronic or electronic form),
  - Actual postage (when the individual has requested that the PHI be mailed), and
  - for preparing an explanation or a summary if agreed to by the individual.

RIGHT OF ACCESS – *FEES*

- The **proposed rule** also specifies that a covered entity may not impose a fee when:
  - an individual inspects his or her own PHI by viewing it, taking notes, photographs or other personal resources to capture the information;
  - an individual accesses EPHI maintained by or on behalf of the covered entity using an internet-based method such as a personal health application, connecting to secure standards-based APIs, consistent with applicable federal or state law.

RIGHT OF ACCESS – *FEES*

- If a covered entity imposes fees, it must provide advance notice.
- The covered entity must post a fee schedule on its website, if it has one, and make the fee schedule available to individuals at the point of service* and upon request. The fee schedule must specify:
  - all types of access to protected health information available free of charge; and
  - Standard fees for:
    - Copies of PHI provided to individuals, with respect to all readily producible electronic and non-electronic forms and formats for such copies;
    - Copies of PHI in an EHR and directed to third parties designated by the individual with respect to any available electronic forms and formats for such copies; and
    - Copies of PHI sent to third parties with the individual's valid authorization under § 164.508, with respect to any available forms and formats for such copies.

Point of service could include at the point of care, at a customer service call center or any location at which PHI is made available for individuals to inspect, including any office responsible for releasing records. Includes orally (over the phone).

RIGHT OF ACCESS – *FEES*

- Upon request, the covered entity must provide (within the initial 15 days):
  - an individualized *estimate* of the approximate fee that may be imposed for providing a copy of the requested PHI for any type of request covered by the required fee schedule.
  - an *itemized* list of the specific charges for labor, supplies, and postage, if applicable, that constitute the total fee charged for any type of request covered by the fee schedule.
- Neither of these requests may automatically extend the time allowed for the covered entity to actually provide the copies of the requested PHI.
  - However, a covered entity would have the ability to inform the individual of one 15-day extension if needed.

RIGHT OF ACCESS – *FEES*

- Fees for ePHI in an EHR directed to a third party would need to be:
  - Reasonable and cost-based if through other than an internet-based method, provided that the fee includes only the cost of:
    - Labor for copying the PHI requested by the individual in electronic form; and
    - Preparing an explanation or summary of the ePHI, if agreed to by the individual.

This category would apply to requests for a copy of PHI that cannot be fulfilled through an automated process. For example, requests to copy PHI in an EHR onto electronic media and mail it to a physical address would fall within this category.

Type of access	Recipient of PHI	Allowable fees
In-person inspection—including viewing and self-recording or -copying	Individual (or personal representative)	Free.
Internet-based method of requesting and obtaining copies of PHI (e.g., using View-Download-Transmit functionality (VDT), or a personal health application connection via a certified-API technology)	Individual	Free.
Receiving a non-electronic copy of PHI in response to an access request	Individual	Reasonable cost-based fee, limited to labor for making copies, supplies for copying, actual postage & shipping, and costs of preparing a summary or explanation as agreed to by the individual.
Receiving an electronic copy of PHI through a non-internet-based method in response to an access request (e.g., by sending PHI copied onto electronic media through the U.S. Mail or via certified export functionality)	Individual	Reasonable cost-based fee, limited to labor for making copies and costs of preparing a summary or explanation as agreed to by the individual.
Electronic copies of PHI in an EHR received in response to an access request to direct such copies to a third party	Third party as directed by the individual through the right of access	Reasonable cost-based fee, limited to labor for making copies and for preparing a summary or explanation agreed to by the individual.

RECAP = Source: 86 Federal Register 6465

RIGHT OF ACCESS – *FEES*

- **No change**: Covered entities are not currently prohibited under the Privacy Rule from requiring individuals to pay a fee for copies of PHI "upfront" before receiving such copies.
- However, OCR continues to encourage covered entities that charge fees for copies of PHI to:
  - waive fees or provide flexibility in payment (such as delaying charges or accepting payment in installments, without delaying the provision of copies) for individuals who are unable to pay upfront due to an emergency or a lack of resources
  - waive access fees in cases where the individual cannot pay the fee due to a demonstrated financial hardship, including when the requesting individual is a Medicaid beneficiary, homeless, otherwise financially disadvantaged, or experiencing financial strain due to some other type of emergency situation.

RIGHT OF ACCESS – *IDENTIFICATION VERIFICATION BURDEN*

- A covered entity may not impose unreasonable identification verification measures on an individual that would impede the individual from exercising their right of access.
- OCR clarifies that unreasonable measures for submitting an access request in writing would be measures that impede the individual from obtaining access when a measure that is less burdensome for individuals is practicable for the particular covered entity.
  - Practicability considerations include:
    - a covered entity's technical capabilities,
    - its obligations to protect the privacy of PHI,
    - the security of EPHI, and
    - the costs of implementing measures that are more convenient for individuals.

RIGHT OF ACCESS – *IDENTIFICATION VERIFICATION BURDEN*

- An unreasonable measure is one that causes an individual to expend unnecessary effort or resources when a less burdensome verification measure is practicable for the covered entity.
- Examples of unreasonable measures include:
  - requiring an individual to provide proof of identity in person when a method for remote verification is practicable for the covered entity and more convenient for the individual;
  - Requiring an individual to obtain notarization of the individual's signature on a written request to exercise the individual right;
  - Requiring individuals to fill out a form with the extensive information contained in a HIPAA authorization form;
  - Requiring that requests for access be made only through the covered entity's online portal; or
  - Applying onerous or infeasible registration requirements for personal health applications or preventing an individual's personal health application from registering with an endpoint (e.g., API) that the covered entity makes public, absent an identified security risk to the ePHI in the covered entity's (or its business associate's) EHR systems.

RIGHT OF ACCESS – *IDENTIFICATION VERIFICATION BURDEN*

- A reasonable measure could be requiring individuals to complete a form with only the limited information needed for the entity to provide access.
  - Reasonable as it only requests information necessary for verification and does not require the individual to expend unnecessary effort.

USES AND DISCLOSURES OF PHI –

- Proposed clarification: OCR would insert language in 45 CFR 164.502(a)(4)(ii),
  - (which currently requires business associates (BAs) to provide copies of PHI to covered entities, individuals, or individuals' designees, to satisfy the covered entity's obligations under the right of access)
- To specify that a BA is required to disclose PHI to the covered entity so the covered entity can meet its access obligations. However, if the BA agreement provides that the BA will provide access to PHI in an EHR directly to the individual or the individual's designee, the BA must then provide such direct access.

PERMITTED DISCLOSURES

- OCR would expressly permit disclosures to Telecommunications Relay Services (TRS) communications assistants for persons who are deaf, hard of hearing, or deaf-blind, or who have a speech disability, and would modify the definition of business associate to exclude TRS providers.

EXPANSION OF THE "MINIMUM NECESSARY" STANDARD

- The minimum necessary standard generally requires covered entities to limit uses and disclosures of PHI to the minimum necessary needed to accomplish the purpose of each use or disclosure.
- The **proposed rule** would create a specific exception for **individual-level** care coordination and case management uses and disclosures regardless of whether such activities constitute treatment or health care operations.

EXPANSION OF THE "MINIMUM NECESSARY" STANDARD

- OCR provides two examples of its reasoning:

1. When a health plan requests a disclosure for care coordination or case management to facilitate an individual's participation in the plan's new wellness program, a requesting health plan or covered health care provider would be relieved of the responsibility for determining the minimum necessary amount of PHI for the purpose and the disclosing health plan or covered health care provider would be relieved of the responsibility of assessing whether reliance on the health plan's determination of the minimum necessary PHI for its purpose is reasonable under the circumstances.

EXPANSION OF THE "MINIMUM NECESSARY" STANDARD

2. When a covered health care provider contacts a health plan to coordinate potential mental health treatment referrals for a patient, the provider would not need to consider what information is the minimum necessary to disclose to the health plan for this purpose.

   – OCR notes that "In fact, the ONC Cures Act Final Rule would prohibit a health care provider from limiting a permissible disclosure to what the provider believes to be the minimum necessary information when the Privacy Rule specifically excepts the disclosure from the minimum necessary standard. However, the provider still could honor an individual's request for restrictions on disclosures of PHI, consistent with the ONC Cures Act Final Rule privacy sub-exception for respecting an individual's request not to share information."

USES AND DISCLOSURES OF PHI – FOR INDIVIDUAL-LEVEL CARE COORDINATION AND CASE MANAGEMENT

- **Proposed Rule**: permissible uses/disclosures would be expanded to expressly permit a covered entity to disclose an individual's PHI to the following:
  - social services agencies,
  - community-based organizations,
  - home and community based services providers, or
  - similar third parties that provide health or human services to specific individuals for individual-level care coordination and case management activities
- No authorization needed.
- The third party does not need to be a health care provider or plan but a provider/ coordinator of ancillary and other health-related services.

USES AND DISCLOSURES OF PHI FOR INDIVIDUAL-LEVEL CARE COORDINATION AND CASE MANAGEMENT

For example:

- a health care provider may disclose the minimum necessary PHI to a senior center or adult day care provider to help coordinate necessary health-related services for an individual, such as arranging for a home aide, to help the older adult or disabled person with their prescribed at-home or post-discharge treatment protocol.
- a disclosure could also facilitate care coordination and case management as part of a covered health plan's health care operations, such as when a health plan discloses the PHI of a senior citizen to a senior wellness center as part of the plan's wellness program in which the senior citizen is enrolled.
- a covered entity could disclose the PHI of a senior individual experiencing chronic illness to a senior center attended by the individual to check on his or her health periodically, and to ask the senior center to give reminders about effective disease self-management.
- A covered entity could disclose PHI to a provider of food or sheltered housing needed to address the individual's health risks.

"PROFESSIONAL JUDGMENT" V. "GOOD FAITH"

- OCR **proposes** to replace the privacy standard that permits covered entities to make certain uses and disclosures of PHI based on their **"professional judgment**" with a standard permitting such uses or disclosures based on a covered entity's **"good faith belief that the use or disclosure is in the best interests of the individual**."
  - More permissive -- presumes a covered entity's good faith.
  - This presumption could be overcome with evidence of bad faith.
- This is to facilitate disclosures to families/other caregivers who are attempting to assist individuals with:
  - health related emergencies,
  - Substance use disorder (SUD-including opioid disorder) or severe mental illness (SMI), and
  - in other circumstances when individuals are incapacitated or otherwise unable to express their privacy preference.

FOR EXAMPLE THE PROPOSED CHANGE WOULD PERMIT:

- A licensed health care professional to draw on experience to make a good faith determination that it is in the best interests of a young adult patient, who has overdosed on opioids, to disclose information to a parent who is involved in the patient's treatment and who the young adult would expect, based on their relationship, to participate in or be involved with the patient's recovery from the overdose.
- Front desk staff at a physician's office who have regularly seen a family member or other caregiver accompany an adult patient to appointments to disclose information about upcoming appointments when the patient is not present, based on the staff's knowledge of the person's involvement and a "good faith" belief about the patient's best interests.
  - front desk staff would not be permitted to decide whether to provide access to records under the individual right of access to a parent who is not their minor child's personal representative.

"PROFESSIONAL JUDGMENT" V. "GOOD FAITH"

- Evidence of bad faith:
  - disclosures for any improper purpose;
  - knowledge that information will be used to harm the individual or will be used for crime, fraud (including defrauding the individual), or personal enrichment;
  - A provider who is sued for malpractice and demands a signed statement of satisfactory care from an incapacitated individual's family member in exchange for disclosing the individual's PHI to the family member.

"PROFESSIONAL JUDGMENT" V. "GOOD FAITH"

- Covered entities still must take into account the facts and circumstances surrounding the disclosures, such as an individual's prior expressed privacy preferences and knowledge of any abusive relationship between the person to whom the covered entity would disclose PHI and the individual.
  - OCR encourages covered entities to ascertain the privacy preferences of individuals who are at known risk of experiencing episodes of incapacity before such individuals become incapacitated, where possible.

"GOOD FAITH"

- The **Proposed Rule** would replace the "professional judgment" standard with "a good faith belief" standard in five regulations:
  1. Unemancipated minors - would permit a covered entity to disclose the PHI of an unemancipated minor to a parent or guardian who is not the personal representative of the individual under HIPAA if consistent with state or other applicable law, provided that such decision is made by a licensed health care professional, based on a **good faith belief** that providing access is in the best interests of the individual. *(45 CFR 164.502(g)(3)(ii)[C]).*

For example, the proposed change would permit a covered health care provider to disclose PHI of an un-emancipated minor experiencing SUD in a state or jurisdiction where applicable law does not treat the minor's parent as a personal representative, when the provider believes that disclosing information to the parent could improve the care and treatment of the minor.

"GOOD FAITH"

2. Use and disclosure for facility directories – would permit a covered entity to include an individual's name in a facility directory and to disclose, for directory purposes, the individual's location and general condition, when the individual is unable to agree or object and the covered entity has a good faith belief that the disclosure is in the best interests of the individual. (*45 CFR 164.510(a)[3]).*

➡ ***For example, this change would facilitate a hospital's disclosure of directory information about an individual who is incapacitated and unable to identify family members or other caregivers involved in his or her care who are trying to locate the individual.***

– The Department does not propose to change the regulation at 45 CFR 164.510(a)(3)(i)(A), which requires that a disclosure under 45 CFR 164.510(a)(3) be consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider.

"GOOD FAITH"

3. Emergency contacts – would to permit covered entities to disclose relevant information to a person involved in the individual's care or payment for care when the covered entity reasonably infers, based on a good faith belief, that the individual does not object. (45 CFR 164.510(b)(2)([ii]).

➡ ***For example, an acute care facility that lacks a written designation of an emergency contact but possesses knowledge of an incapacitated patient's designated emergency contact could disclose PHI to that contact, based on a good faith belief that the patient does not object to the disclosure.***

– In contrast, a disclosure of PHI by a covered entity with knowledge of an individual's advance directive that documents an objection to disclosure to a particular person would be inconsistent with a good faith belief that the individual does not object.

"GOOD FAITH"

4. Limited uses and disclosures when the individual is not present - would permit covered entities to disclose relevant information about the individual to family members and other caregivers who are involved with the individual's care or payment for care, or who require notification related to the individual, when the individual cannot agree to the disclosure because of absence, incapacity, or emergency circumstances, and the covered entity has a good faith belief that the disclosure is in the best interests of the individual. *(45 CFR 164.510(b)[3]).*

➡ ***For example, this change would facilitate a health care provider's disclosure of PHI to a caregiver of a patient who is incapacitated by an overdose, mental health crisis, or other health emergency.***

- The Privacy Rule does not define incapacity and a formal determination is not necessary. OCR has provided examples in prior guidance:
  - unconscious
  - suffering from temporary psychosis or
  - under the influence of drugs or alcohol

  See https://www.hhs.gov/hipaa/for-professionals/faq/2090/when-does-mental-illness-or-another-mental-condition-constitute-incapacity-under-privacy-rule.html

"GOOD FAITH"

5. Verification requirements – would provide that a covered entity would satisfy its obligations to verify a requestor's identity if the covered entity acts on a good faith belief in making a disclosure of relevant PHI. (45 CFR 164.514(h)(2)[iv]).
   - Such disclosures are already limited in scope to the information relevant to assisting the individual with his or her health care or payment for care or to the minimum amount of information necessary for the purpose.

➡ ***For example, this proposal would improve the ability of a covered hospital to disclose PHI of an individual experiencing an emergency to a person who represents that he or she is a family member or caregiver of the individual, without requiring the family member or caregiver to present documentation of the relationship with the individual, if the hospital has a good faith basis for believing the requestor and the requestor's identity.***

➡ ***A hospital may not have a good faith basis for believing the requestor's representations about the requestor's identity and relationship with the individual if a workforce member receives a request from an unfamiliar and unverified email address or the requestor is unknown and not named as a contact in an individual's record.***

"SERIOUS AND IMMINENT" V. "SERIOUS AND REASONABLY FORESEEABLE"

- OCR would expand the ability of covered entities to disclose PHI to avert a threat to health or safety when harm is **"serious and reasonably foreseeable**," instead of the current stricter standard which requires a "**serious and imminent**" threat to health or safety.
  - As always, the recipient of the PHI must be reasonably able to prevent harm or lessen the threat, or the use or disclosure must be necessary for law enforcement to identify or apprehend an individual.
- OCR recognizes that it is not always possible to determine if harm is "imminent."

"SERIOUS AND REASONABLY FORESEEABLE"

- The **Proposal** would define "reasonably foreseeable" as when an ordinary person could conclude that a threat to health or safety exists and that harm to health or safety is reasonably likely to occur if a use or disclosure is not made, based on facts and circumstances known at the time of the disclosure.
  - Determinations made by a licensed mental or behavioral health professional - or other providers who have specialized training, expertise, or experience in assessing an individual's risk to health or safety — will be entitled to heightened deference.

"SERIOUS AND REASONABLY FORESEEABLE"

- The "reasonably foreseeable" standard involves consideration of whether a similarly situated covered entity could believe that a serious harm is reasonably likely to occur, and does not require a determination that a majority of covered entities could have such a belief.
  - Assumptions unwarranted by the individual's diagnosis and specific circumstances would not meet the standard.

➡ ***For example, the assumption that a person with a diagnosis of depression or anxiety is a threat to themselves or others merely by virtue of that diagnosis is unfounded.***

➡ ***Assuming that an individual on the autism spectrum who displays certain behaviors frequently associated with mental illness has co-occurring mental illness without any such diagnosis is unfounded.***

"SERIOUS AND REASONABLY FORESEEABLE"

- Threats to public health or safety might include:
  - mass shootings,
  - the use of explosive devices to attack a crowd, or
  - other acts of terrorism.

➡ For an individual who poses a threat to public safety, a "serious and reasonably foreseeable threat" standard may afford a health care provider sufficient time to notify a person, such as a law enforcement official, who is in a position to avert a serious harm that may occur and ensure the safety of the individual and others.

➡ A "reasonably foreseeable threat" standard could further enable a health care provider to timely notify a family member that an individual is at risk of suicide, even if the provider cannot predict that a suicide attempt is likely to occur "imminently."

"SERIOUS AND REASONABLY FORESEEABLE"

- OCR stresses that these examples are intended to highlight for covered health care providers their ability to use or disclose PHI to lessen the threat of, or prevent harm due to, potential mass violence.
- Covered entities (or a member of a covered entity's workforce) need not have such specialized training, expertise, or experience in order to meet the reasonably foreseeable standard.

NOTICE OF PRIVACY PRACTICES (NPP)

- The **proposal** would eliminate the requirement that direct treatment provider's obtain an individual's written acknowledgment of receipt of the provider's NPP.
  - to ensure that individuals are able to understand and make decisions based on the information in the NPP, the proposal would replace the written acknowledgment requirements with an individual right to discuss the NPP with a person designated by the covered entity.

NOTICE OF PRIVACY PRACTICES (NPP)

- The **proposal** would also modify the content requirements of the NPP to clarify for individuals their rights with respect to their PHI and how to exercise those rights.
  - The required header of the NPP would be modified to specify to individuals that the notice provides information about:
    - how to access their health information;
    - how to file a HIPAA complaint; and
    - individuals' right to receive a copy of the notice and to discuss its contents with a designated person.

The required header would specify whether the designated contact person is available onsite and must include a phone number and email address the individual can use to reach the designated person.

NOTICE OF PRIVACY PRACTICES (NPP)

- The **proposal** would modify the required element of an NPP that addresses the access right:
  - to describe how an individual can exercise the right of access to obtain a copy of their records at limited cost (or, in some cases, free of charge), and
  - to direct a covered health care provider to transmit an electronic copy of PHI in an EHR to a third party.
- The **proposal** would add an optional element to the NPP to include information to address instances in which individuals seek to direct their PHI to a third party, when their PHI is not in an electronic health record or is not in an electronic format.
  - Purpose = help make individuals aware that they retain the right to obtain the PHI directly and give it to a third party or they can request to send a copy of PHI directly to a third party using a valid authorization.

GW | GARFUNKEL WILD, P.C. ATTORNEYS AT LAW

QUESTIONS?

CONTACT INFORMATION

Robert A. Del Giorno, Esq.
516.393.2505
rdelgiorno@garfunkelwild.com

Kathleen M. Brown, Esq.
518.560.4023
kbrown@garfunkelwild.com

677 Broadway
Albany, NY 12207
(518) 242-7582

111 Great Neck Road
Great Neck, NY 11021
(516) 393-2200

350 Bedford Street
Stamford, CT 06901
(203) 316-0483

411 Hackensack Ave.
Hackensack, NJ 07601
(201) 883-1030