ADVISORY OPINION 21-04—HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (1) PERMISSIBLE ANNUAL PENALTIES, (2) REQUIREMENT THAT PENALTIES BE PROPORTIATE, REASONABLE, AND CONSISTENT, (3) FAILURE TO COOPERATE AS A SEPARATE VIOLATION, AND (4) MEANING OF "FINANCIAL INSTITUTION"

This Advisory Opinion addresses a number of disparate issues arising under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA" or "Act"). First, we explain the rationale underlying our recommendation, implemented by the Office for Civil Rights that the penalty table issued in 74 Fed. Reg. 56,123 (Oct. 30, 2009) was contrary to law and should not be enforced. *See* 84 Fed. Reg. 18,151 (April 30, 2019) (Notice exercising enforcement discretion). This conclusion was recently confirmed by the Fifth Circuit in *University of Texas Cancer Center v. United States Department of Health and Human Services*, No. 19-60226 (Jan. 14, 2021) ("*M.D. Anderson*"). Second, in light of *M.D. Anderson* we emphasize the need for consistency and rationality when assessing penalties. Third, we analyze whether "failure to cooperate" during an OCR investigation constitutes a separate violation of the Act or its implementing regulations. Fourth, we assess the scope of the "financial institution" exception to putative business associates.

I. ENFORCEMENT REGULATION IS INCONSISTENT WITH HITECH

On April 30, 2019, the Office for Civil Rights ("OCR") indicated that, based on an opinion from the Office of the General Counsel, it would exercise its enforcement discretion with respect to the penalties that it would assess under the Health Information Technology for Economic and Clinical Health (HITECH Act), enacted as part of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115, 226 *et seq*. (Feb. 17, 2009) ("ARRA"). *See* 84 Fed. Reg. 18,151 (April 30, 2019). We concluded that the penalties set out in the original regulation were inconsistent with HITECH and according to the Notice, did not represent the "best reading" of the statute. Since that publication, this Office has received requests, including from Congress, to further articulate the basis for our view that the set of penalties in the original rule initially issued on October 30, 2009, is inconsistent with HITECH. *See* 74 Fed. Reg. 56,123 (Oct. 30, 2009). It should be noted that OGC's views were confirmed by the *M.D. Anderson* court.

Background:

The ARRA, through HITECH, enhanced penalties for violating the administrative

simplification provisions of HIPAA.[1] For such violations, the new regime required tiered penalties based on the actor's state of mind. Thus, if the person were unaware that he or she violated HIPAA and through due care would not have known, the Secretary imposes "a penalty for each such violation of an amount that is at least the amount described in paragraph (3)(A) but not to exceed the amount described in paragraph (3)(D)[.]" Social Security Act § 1176(a)(1)(A) (emphasis supplied). Where the violation was due to reasonable cause, the Secretary imposes "a penalty for each such violation of an amount that is at least the amount described in paragraph (3)(B) but not to exceed the amount described in paragraph (3)(D)[.]" *Id*. at § 1176(a)(1)(B) (emphasis supplied). If the violation were due to willful neglect but is corrected, the Secretary imposes "a penalty in an amount that is at least the amount described in paragraph (3)(C) but not to exceed the amount described in paragraph (3)(D)[.]" *Id*. at § 1176(a)(1)(C)(i) (emphasis supplied). And finally, if the violation were due to willful neglect but was not corrected, the Secretary imposes "a penalty in an amount that is at least the amount described in paragraph (3)(D)." *Id*. at § 1176(a)(1)(C)(ii) (emphasis supplied).

The actual penalties are set out in paragraph (3):

> Tiers of penalties described.—For purposes of paragraph (1), with respect to a violation by a person of a provision of this part—
>
> (A) the amount described in this subparagraph is $100 for each such violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $25,000;
> (B) the amount described in this subparagraph is $1,000 for each such violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $100,000;
> (C) the amount described in this subparagraph is $10,000 for each such violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $250,000; and
> (D) the amount described in this subparagraph is $50,000 for each such violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $1,500,000.

Id. at § 1176(a)(3).

On October 30, 2009, the Secretary issued an interim final rule ("IFR" or "Enforcement Rule") implementing the above penalty provisions of HITECH. *See* 74 Fed. Reg. 56,123 (Oct. 30, 2009). The IFR claimed that HITECH's penalty provisions were "conflicting" in that they

[1] The amendments are set out in division A, Title XIII, Subtitle D and are known as the 'Health Information Technology for Economic and Clinical Health Act'' or the ''HITECH Act.''

"reference[] two tiers of penalties 'for each violation,' which each provide a penalty amount 'for all such violations' of an identical requirement" in a calendar year. *Id*. at 56,127 (col. b). As a result, the IFR adopted a per violation upper limit of $50,000 for each of the four tiers and an annual limit of $1,500,000 for each of the four tiers. It read out of the statute the $25,000, $100,000, and $250,000 yearly cumulative limits.

Analysis:

It is by now axiomatic that "[i]f the intent of Congress is clear, that is the end of the matter; for the court, as well as the agency, must give effect to the unambiguously expressed intent of Congress." *Chevron, U.S.A., Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837, 842–43 (1984). Here, the penalty provisions are not ambiguous and the IFR points to no ambiguity. Rather it claims that the language is "conflicting" but again, pointed to no such conflict. There is nothing ambiguous about the provision.

Each of the four mental states references a range of penalties per violation with a constant upper limit and each of the four has a separate cumulative annual limit. Therefore, the statute provides the following penalty matrix[2]:

Culpability		Minimum penalty/ violation	Maximum penalty/ violation	Annual limit
No Knowledge		$100	$50,000	$25,000
Reasonable Cause		1,000	50,000	100,000
Willful Neglect—Corrected		10,000	50,000	250,000
Willful Neglect—Not Corrected		50,000	50,000	1,500,000

In contrast, the IFR uses a constant annual upper limit of $1.5 million for each of the four states of mind. This presents two problems. First, it is not what the statute says and second, it reads out of the statute the $25,000, $100,000 and $250,000 annual upper limits. The statute is straightforward, both structurally and linguistically. Paragraph (1) relates solely to per violation offenses and describes the state of mind for each type of violation. It does not directly set penalties, but rather cross-references "an amount that is at least the amount described in" the corresponding cross-referenced subparagraph of paragraph (3) and an upper limit as described in paragraph 3(D). Paragraph (1) does not describe or otherwise allude to annual limits. In contrast, paragraph (3) sets out the lower limits per violation for each infraction as well as an upper, annual limit for each type of infraction. Critically, paragraph (3) sets out four distinct annual limits, depending on the nature of the infraction.

How the IFR ordained a constant annual limit for each state of mind raises serious

[2] HHS is required to annually adjust its CMPs for inflation pursuant to the cost-of-living formula set forth in the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015, enacted as part of the Bipartisan Budget Act of 2015, Pub. L. No. 114-74, section 701, 129 Stat. 599 (Nov. 2, 2015).

concerns. While we recognize that the above matrix has an anomaly, namely that the upper limit per violation for the first state of mind is more than the annual limit for that state of mind, that anomaly is not an ambiguity, nor is it an inconsistency. It does not authorize a wholesale rewriting of the statute by regulation. Specifically, the $50,000 per violation upper limit and the $25,000 annual limit for the first state mind of are not inconsistent. The upper limit proviso merely states that the upper limit per violation is "not to exceed the amount described in paragraph (3)(D)[.]" There is nothing that compels an upper limit of $50,000 for the first state of mind; rather, the penalty shall not exceed $50,000; a $25,000 annual limit does not exceed $50,000. Therefore, credence can be given to both.

Credence, though, cannot be given to the IFR, which appears to be inconsistent "with one of the most basic interpretive canons," namely "that [a] statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant." *Rubin v. Islamic Republic of Iran*, ___U.S.___, 138 S. Ct. 816, 824–25 (2018) (quoting *Corley v. United States*, 556 U.S. 303, 314, (2009)) (internal quotation marks omitted). "As this Court has noted time and time again, the Court is 'obliged to give effect, if possible, to every word Congress used.' *Reiter v. Sonotone Corp*., 442 U.S. 330, 339 (1979)." *National Ass'n of Mfrs. v. Department of Defense*, ___U.S.___, 138 S. Ct. 617, 632 (2018). *See also New York v. E.P.A.*, 443 F.3d 880, 887 (D.C. Cir. 2006) ("Only in a Humpty Dumpty world would Congress be required to use superfluous words while an agency could ignore an expansive word that Congress did use. We decline to adopt such a world-view."). Here, the IFR excised three annual limits when translating the statute into the IFR; no reason was given for treating these provisions as superfluous. As such, in our view, the regulation's three upper annual limit provisions are invalid and cannot be enforced.

Our reading is not just the "best reading" of HITECH, it is the only reading, a conclusion mirrored by the *M.D. Anderson* court when it recently noted that the interpretation set out in the original rule was "indefensib[le]" and that it "nonsensically conflate[ed] the fault levels specified by Congress." *See M.D. Anderson*, slip at 13-14 n.5.

II. OCR'S PENALTIES MUST BE CONSISTENTLY APPLIED AND RATIONALLY BASED

We have received inquiries about whether the process that OCR uses to assess penalties is cabined by regulation. As discussed below, it is. HIPAA's implementing regulation requires OCR to consider various factors in assessing penalties for violations, as follows:

> In determining the amount of any civil money penalty, the Secretary will consider the following factors, which may be mitigating or aggravating as appropriate:
>
> (a) The nature and extent of the violation, consideration of which may include but is not limited to:
>
> (1) The number of individuals affected; and
> (2) The time period during which the violation occurred;

(b) The nature and extent of the harm resulting from the violation, consideration of which may include but is not limited to:

(1) Whether the violation caused physical harm;
(2) Whether the violation resulted in financial harm;
(3) Whether the violation resulted in harm to an individual's reputation; and
(4) Whether the violation hindered an individual's ability to obtain health care;

(c) The history of prior compliance with the administrative simplification provisions, including violations, by the covered entity or business associate, consideration of which may include but is not limited to:

(1) Whether the current violation is the same or similar to previous indications of noncompliance;
(2) Whether and to what extent the covered entity or business associate has attempted to correct previous indications of noncompliance;
(3) How the covered entity or business associate has responded to technical assistance from the Secretary provided in the context of a compliance effort; and
(4) How the covered entity or business associate has responded to prior complaints;

(d) The financial condition of the covered entity or business associate, consideration of which may include but is not limited to:

(1) Whether the covered entity or business associate had financial difficulties that affected its ability to comply;
(2) Whether the imposition of a civil money penalty would jeopardize the ability of the covered entity or business associate to continue to provide, or to pay for, health care; and
(3) The size of the covered entity or business associate; and

(e) Such other matters as justice may require.

45 C.F.R. § 160.408.

In all, OCR is required, under its own regulations, to consider twelve sub-factors and one factor (referred to collectively as "factors") in assessing penalties and it must do so consistently. *See Delaware Riverkeeper Network v. F.E.R.C.*, 753 F.3d 1304, 1313 (D.C. Cir. 2014) ("In determining whether agency action is arbitrary and capricious, courts consider whether the decision was 'based on a consideration of the relevant factors'" (quoting *Motor Vehicle Mfrs. Ass'n of the U.S., Inc. v. State Farm Mut. Auto. Ins.*, 463 U.S. 29, 43, (1983)).[3] The *M.D. Anderson* court cast doubt on whether OCR in fact applied these factors to yield uniform and consistent

[3] On January 5, 2021, Pub. L. No. 116-321 amended HITECH to also require the Secretary to consider certain recognized security practices of covered entities and business associates when making civil money penalty determinations, and for other purposes.

results, finding that "an administrative agency cannot hide behind the fact-intensive nature of penalty adjudications to ignore irrational distinctions between like cases." *M.D. Anderson* at slip op. 12.

OCR must provide reasoned analyses demonstrating that it applied all thirteen factors consistently across cases. This requirement derives not only from basic principles of administrative law but also from principles of substantive due process that precludes the government from acting arbitrarily, especially when setting penalties. The hallmark of arbitrary and capricious behavior is the imposition of penalties willy-nilly where it is difficult to fathom the bases for the observed differences. The regulations require a rational relationship between the harm, no matter how characterized, and the penalty. So does the Fifth Amendment. "The Due Process Clause of the Fourteenth Amendment prohibits the imposition of grossly excessive or arbitrary punishments." *State Farm Mut. Auto. Ins. Co. v. Campbell*, 538 U.S. 408, 416 (2003). The Eighth Amendment, as applied to the federal government, is no less protective: "The amount of the [fine] must bear some relationship to the gravity of the offense that it is designed to punish." *United States v. Bajakajian*, 524 U.S. 321, 334 (1998). The Supreme Court's seminal case, *BMW of North America Inc. v. Gore*, 517 U.S. 559 (1996), provides the constitutional test for whether punitive damages, and by analogy civil money penalties, are excessive. It instructs courts to consider three guideposts: "(1) the degree of reprehensibility of the defendant's misconduct; (2) the disparity between the actual or potential harm suffered by the plaintiff and the punitive damages award; and (3) the difference between the punitive damages awarded by the jury and the civil penalties authorized or imposed in comparable cases." *State Farm*, 538 U.S. at 418 (citing *Gore*, 517 U.S. at 575); *see Burke v. Regalado*, 935 F.3d 960, 1037 (10th Cir. 2019). The four primary factors set out in the regulations (subsections (a) through (d)) and their constituent sub-factors capture these three constitutional guideposts.

The regulation, however, must be applied; it is not there for window dressing nor to provide a basis to rationalize a pre-ordained result. Rather, all of the factors must be used by the agency to calculate the penalty. Attempting to justify a penalty pulled from thin air by applying the thirteen factors in such way as to "back into" the penalty is the operational definition of arbitrary and capricious agency action. Accordingly, the administrative record in any penalty case under HIPAA must include the agency's analysis of the thirteen factors leading to the penalty sought. Articulating the basis for any penalty is particularly important where the agency is permitted by statute to supplement its HIPAA-enforcement budget with penalties that it collects thereby creating appearance of a conflict (*see* 42 USC § 17939), albeit condoned by Congress.

In short, it is the view of the General Counsel that OCR may not assess penalties as cudgel to beat a litigant into submission, but must assess penalties in a rational and consistent manner taking into account each of the thirteen factors required by the agency's rules and the factors required by the Constitution.

III. OCR MAY NOT IMPOSE PENALTIES FOR FAILURE TO COOPERATE

Questions have been raised as to whether OCR may properly impose penalties if a respondent fails to "cooperate" with OCR in the course of its investigation. For the reasons set forth below, neither HIPAA nor HITECH authorize OCR to impose such penalties.

The regulation, under a provision entitled "Responsibilities of covered entities and business associates," provides, in relevant part, as follows:

> A covered entity or business associate must cooperate with the Secretary, if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of the covered entity or business associate to determine whether it is complying with the applicable administrative simplification provisions.

45 C.F.R. § 160.310(b).

It is axiomatic that an agency's power to promulgate legislative regulations is limited to the authority delegated to it by Congress. *See Bowen v. Georgetown Univ. Hosp*., 488 U.S. 204, 208 (1988); *Merck & Co., Inc. v. U.S. Dep't of Health and Human Servs.*, 931 F.3d 531 (D.C. Cir. 2020); *Bayou Lawn & Landscape Servs. v. Sec'y of Labor*, 713 F.3d 1080 (11th Cir. 2013). If the agency lacks congressional authority to issue a particular rule, that rule is void *ab initio*. At issue here is whether section 160.310, which mandates cooperation, is authorized by Congress.

"[O]ur inquiry begins with the statutory text, and ends there as well if the text is unambiguous." *BedRoc Ltd., LLC v. United States*, 541 U.S. 176, 183 (2004). The penalty provision of HIPAA authorizes the Secretary to impose penalties "on any person who violates a provision of this part" [C] of title 11. Social Security Act § 1176(a). The plain text of HIPAA only authorizes the Secretary to impose penalties for a violation of HIPAA itself. HIPAA requires covered entities and business associates to hew to various standards for handling a person's protected health information. Specifically, the grant of rulemaking authority states as follows:

> (1) IN GENERAL.—If legislation *governing standards with respect to the privacy of individually identifiable health information* transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by the date that is 36 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall promulgate final regulations *containing such standards* not later than the date that is 42 months after the date of the enactment of this Act. Such regulations shall address at least the subjects described in subsection (b).

HIPAA § 264(c) (emphasis supplied).

The term "standard" relates to data elements, including code sets, financial transactions, and security measures to safeguard patient data. *See* SSA §§ 1171(7), 1172-1175. The plain text of

the statute cabins the Secretary's rulemaking authority to adopting "standards." The organic legislation does not authorize the Secretary to impose other forms of requirements, such as cooperation, but to the contrary restricts the Secretary's rulemaking authority to "standards." "Congress knows to speak in plain terms when it wishes to circumscribe, and in capacious terms when it wishes to enlarge agency discretion." *Ciox Health v. Azar*, 435 F. Supp. 3d 30, 64 (D.D.C. 2020) (quoting *City of Arlington, Tex. v. FCC*, 569 U.S. 290, 296 (2013)). Here, Congress did not speak in capacious terms, but instead specified with precision what can be included in the regulations.

Nor is the Secretary's general rulemaking authority (which was not initially included as a statutory authority for § 160.310(b)) sufficient to provide authorization to expand on the rulemaking authority granted by HIPAA. Under section 1102(a), the Secretary is authorized to issue rules "as may be necessary to the efficient administration of the functions with which each is charged under this Act." The D.C. Circuit held that, for a regulation to be "necessary" to the program's "administration," a requisite of section 1102, the Secretary "must demonstrate an actual and discernible nexus between the rule and the conduct or management of Medicare and Medicaid programs." *Merck & Co., Inc.*, 962 F.3d at 538. That court recently ruled that section 1102 does not authorize the Department's regulation requiring drug manufacturers to disclose in their television advertisements the wholesale acquisition cost of many prescription drugs and biological products for which payment is available under Medicare or Medicaid, even though the rule would improve the efficiency of Medicare and Medicaid programs by reducing wasteful and abusive increases in drug product list prices. Here, the regulation would impose penalties for non-cooperation, something the rule in *Merck* did not do. Section 160.310(b) is therefore arguably further removed from what is permitted under section 1102.

More critically, though, a general grant of rulemaking authority is normally insufficient to enlarge a more restricted grant of specific authority. It is a fundamental maxim of statutory interpretation that a statute of specific intention takes precedence over one of general intention. *See Morales v. Trans World Airlines*, 504 U.S. 374, 384 (1992); *Sierra Club–Black Hills Group v. United States Forest Serv.*, 259 F.3d 1281, 1287 (10th Cir. 2001). Here HIPAA authorizes the Secretary to issue regulations to implement some, but not all, of its provisions. The grant of general authority cannot enlarge on that more prescribed grant of authority. This is especially the case where the regulatory requirement it creates is not found in the statute and carries with it significant financial penalties.

The statutory context further confirms this interpretation. Elsewhere in the Social Security Act, Congress evidently knew how to grant the Secretary authority to require cooperation. Indeed, in the same title of the Social Security Act as HIPAA, Congress required persons "to grant timely access, upon reasonable request (as defined by the Secretary in regulations) to any of the" Secretary to the Inspector General, and to a Medicaid fraud unit to review records relating to Medicaid payments. Social Security Act § 1128(a)(12); *see also* Social Security Act § 1128A (subjecting to civil monetary penalties any person who "fails to grant timely access, upon reasonable request (as defined by the Secretary in regulations), to the Inspector General of the Department of Health and Human Services, for the purpose of audits, investigations, evaluations, or other statutory functions of the Inspector General of the Department of Health and Human Services"). The Part D program has a comparable cooperation

requirement. *See id*. § 1860D-27(d)(2). When Congress wanted to mandate cooperation, it knew what words to use. Those words are missing from HIPAA. "Where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion." *Barnhart v. Sigmon Coal Co*., 534 U.S. 438, 452 (2002); *Russello v. United States*, 464 U.S. 16, 23 (1983).

Had Congress wanted to impose a requirement of cooperation on entities, many of which are not tied to the Department by the Spending Clause, it knew how to word the provision, but instead omitted it. Its absence strongly suggests that Congress had no intention of imposing this additional requirement on those falling within HIPAA's ambit. As such, we conclude that the rule requiring cooperation (*i.e*., 45 C.F.R. § 160.310) is not authorized by either HIPAA or HITECH and therefore is not a requirement that would subject a respondent to civil money penalties.

IV. CERTAIN ACTIVITIES OF THE TYPE PERFORMED BY A FINANCIAL INSTITUTION ARE EXEMPT FROM HIPAA AND HITECH

HHS has for many years received questions about the scope and meaning of section 1179 of the Social Security Act (42 U.S.C. § 1320d–8).[4] Section 1179 exempts certain activities of a financial institution from HIPAA. Below we set forth some general principles for determining when certain conduct falls within this exemption.

Section 1179 provides in relevant part:

> To the extent that *an entity is engaged in activities of a financial institution* (as defined in section 3401 of Title 12)[5], or is engaged in authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments, for a financial institution, this part, and any standard adopted under this part, shall not apply to the entity with respect to such activities, including the following:
>
> > **(1)** The use or disclosure of information by the entity for authorizing, processing, clearing, settling, billing, transferring, reconciling or collecting, a payment for, or related to, health plan premiums or health care, where such payment is made by any means,

[4] *See, e.g.*, Letter from Lumpkin (National Committee on Vital and Health Statistics) to Sec. Thompson (June 17, 2004), available at https://perma.cc/K7E5-K4NB; Letter from Suarez (National Committee on Vital and Health Statistics) to Sec. Thompson (Sept. 16, 2015), available at https://perma.cc/APF8-A2H3.

[5] Section 3401 defines a "financial institution" as "any office of a bank, savings bank, card issuer . . . industrial loan company, trust company, savings association, building or homestead association (including cooperative banks), credit union, or consumer finance institution, located in any state or territory of the United States." 12 U.S.C. § 3401(1).

> including a credit, debit, or other payment card, an account, check, or electronic funds transfer.

Social Security Act § 1179 (emphasis supplied).

An entity need not be a financial institution to fall within Section 1179's exemption; the entity simply "must engage in activities of a financial institution" (or on behalf of a financial institution). Were it otherwise, Congress would have used the words "financial institution" instead of "entity" in the first clause of Section 1179. Moreover, the activities described in section 1179(1)-(2) are a non-exhaustive list of activities that are exempt under Section 1179.

Both the HIPAA and HITECH regulations are consistent with the premise that an entity that engages in the activities set forth in section 1179 is exempt from HIPAA, the HIPAA regulations, and the HITECH regulations. The HIPAA Privacy Rule preamble explained:

> We interpret section 1179 of the Act to mean that entities engaged in the activities of a financial institution, and those acting on behalf of a financial institution, are not subject to this regulation when they are engaged in authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments for a financial institution.

65 Fed. Reg. 82,570.

The HITECH regulations did not purport to change the implementation or interpretation of Section 1179. *See* 78 Fed. Reg. 5566, 5575 (Jan. 25, 2013) ("This final rule is not intended to affect the status of financial institutions with respect to whether they are business associates. The HIPAA Rules, including the business associate provisions, do not apply to banking and financial institutions with respect to the payment processing activities identified in § 1179 of the HIPAA statute").

Thus, the section 1179 exemption applies so long as an entity is engaged in the activities set forth in section 1179. For example, under the plain text of 1179, a payment gateway is exempt from HIPAA when it engages in processing payments, including but not limited to credit card or debit card transactions.

There appears to be some confusion about whether an entity engaged in the activities of a financial institution is subject to HIPAA when it acts on behalf of a covered entity. But under HIPAA and the HIPAA regulations, entities engaged in the activities of a financial institution described in section 1179 are exempt, regardless of whether those activities in some way benefit the covered entity. The HIPAA Privacy Rule's preamble stated:

> We interpret this provision to mean that when a financial institution, or its agent on behalf of the financial institution, conducts the activities described in section 1179, the privacy regulation will not govern the activity.

> If, however, these activities are performed by a covered entity or by another entity, including a financial institution, on behalf of a covered entity, the activities are subject to this rule. For example, if a bank operates the accounts payable system or other "back office" functions for a covered health care provider, that activity is not described in section 1179. In such instances, because the bank would meet the rule's definition of "business associate," the provider must enter into a business associate contract with the bank before disclosing protected health information pursuant to this relationship. However, if the same provider maintains an account through which he/she cashes checks from patients, no business associate contract would be necessary because the bank's activities are not undertaken for or on behalf of the covered entity, and fall within the scope of section 1179. In part to give effect to section 1179, in this rule we do not consider a financial institution to be acting on behalf of a covered entity when it processes consumer-conducted financial transactions by debit, credit or other payment card, clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for compensation for health care.

65 Fed. Reg. 82,461, 82,571 (Dec. 28, 2000).

This passage did not purport to provide that Section 1179 automatically does not apply when activities of a financial institution benefit a covered entity or are performed on behalf of a covered entity. Such an interpretation would have run afoul of the statutory exemption. The examples provided of acting on behalf of a covered entity—operating accounts payable or "back office" activities for the covered entity—are examples of activities that could at times be outside the scope of Section 1179, not because they are performed on behalf of a covered entity, but because they are not activities of a financial institution. Operating accounts payable or certain back office activities might (at least in some cases) not constitute exempt activities such as **"**authorizing, processing, clearing, settling, billing, transferring, reconciling or collecting, a payment for, or related to, health plan premiums or health care.**"** Social Security Act § 1179(1).

We interpret the preamble language this way to avoid a conflict with the statute. If an entity engages in the activities described in section 1179, HIPAA, the HIPAA regulations, and the HITECH regulations do not apply, irrespective on whose behalf the activities might be performed.

Limitations:

For these reasons, the Office of the General Counsel concludes that the original penalty rule as issued and readopted are inconsistent with the organic legislation, that all thirteen factors spelled out in the Secretary's regulations must be applied and applied consistently when assessing penalties, that the regulation requiring cooperation during an OCR investigation or audit is not authorized by HIPAA or HITECH and finally, the so-called financial institution

exception applies to both financial institutions and other entities that are engaged in the delineated activities of a financial institution.

This Advisory Opinion may be supplemented or modified by the Office of the General Counsel. It is intended to minimize the need for individual advisory opinions. This Advisory Opinion sets forth the current views of the Office of the General Counsel.[6] It is not a final agency action or a final order, and it does not have the force or effect of law.

//s//

Robert P. Charrow
General Counsel
January 19, 2021

[6] *See Air Brake Sys., Inc. v. Mineta*, 357 F.3d 632, 647–48 (6th Cir. 2004) (holding that the Chief Counsel of the National Highway Traffic Safety Administration had delegated authority to issue advisory opinions to regulated entities in fulfillment of a congressional directive to promote regulatory compliance); 5 U.S.C. § 301 ("The head of an executive department . . . may prescribe regulations for the government of his department, the conduct of its employees, [and] the distribution and performance of its business[.]"); *Statement of Organization, Functions, and Delegations of Authority*, 85 Fed. Reg. 54,581, 54,583 (Sept. 2, 2020).