Case No. 13-15324

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

NICK COONS, et al.,
Plaintiffs-Appellants,

vs.

JACOB J. LEW (in his official capacity as Secretary of the United States Department of the Treasury), et al.,
Defendants-Appellees.

APPELLANTS' REPLY BRIEF

Appeal from the United States District Court for the State of Arizona
Case No. 2:10-CV-1714-GMS, Hon. Murray Snow, presiding

Clint Bolick
Kurt Altman
Nicholas C. Dranias
Christina Sandefur
GOLDWATER INSTITUTE
Scharf-Norton Ctr. for Const. Lit.
500 E. Coronado Rd.
Phoenix, AZ 85004
P: (602) 462-5000/F: (602) 256-7045
cbolick@goldwaterinstitute.org
kaltman@goldwaterinstitute.org
ndranias@goldwaterinstitute.org
csandefur@goldwaterinstitute.org
Attorneys for Appellants

TABLE OF CONTENTS

TABLE OF AUTHORITIES

ARGUMENT

I. Coons has a constitutional right to medical autonomy and has stated a claim that PPACA unduly burdens that right.

The district court erred in refusing to recognize Nick Coons' due process right to medical autonomy. This Court should reverse the dismissal and allow Coons to show that the Patient Protection and Affordable Care Act (PPACA) burdens this right by forcing him to buy government-sanctioned health insurance that he does not want or pay the penalty for refusing to do so, thereby displacing and reducing the health care treatments and patient-doctor relationships he can afford. ER53-54 ¶ 16; ER69 ¶¶ 83-85.

The government does not appear to endorse the district court's grounds for dismissing Coons' medical autonomy claim; namely, the court's refusal to recognize "a substantive due process right to choose medical providers and treatment." ER6. Nor could it, since Coons has shown that such a right is firmly rooted in this Court's precedents. *See* Appellants' Opening Brief ("Opening Brief") pp. 16-17. Instead, the government contends that it may avoid constitutional concerns so long as it affords Coons the option to pay a penalty in exchange for exercising this constitutional right. *See* Appellees' Response ("Response") pp. 9-10. Yet this begs the question. The Constitution does not allow the government "needlessly [to] encourage[] the waiver of constitutional rights," *United States v. Chavez*, 627 F.2d 953, 956 (9th Cir. 1980), *cert. denied*, 101 S. Ct. 1376 (1981), or

to impose significant financial penalties on the exercise of constitutional rights. *See id.* at 955-57; *United States v. Frierson*, 945 F.2d 650, 658-59 (3d Cir. 1991).

The government maintains that Coons' medical autonomy concerns are unworthy of protection because "[t]he Supreme Court long ago abandoned the protection of economic rights through substantive due process." Response p. 10 (*quoting U.S. Citizens Ass'n v. Sebelius*, 705 F.3d 588, 601 (6th Cir. 2013)).[1] But Coons does not assert an "economic right." Although the tax penalty is financial, the injury is to his personal liberty right to medical autonomy and to his choice of medical care.[2] The tax "seeks to shape [individual] decisions about whether to buy health insurance," *Nat'l Fed'n of Indep. Bus. v. Sebelius* ("*NFIB*"), 132 S. Ct. 2566, 2596 (2012), and it forces Coons to choose between yielding his decision-making regarding such intensely personal matters as preferred health care procedures and doctor-patient relationships to a private insurance company, or paying a significant financial penalty. ER53-54 ¶ 16; ER68-69 ¶¶ 80-86. Thus Coons' injury is to his fundamental liberty and triggers strict scrutiny. *Kramer v.*

[1] *U.S. Citizens Ass'n* is not binding on this Court, nor is it helpful in deciding this issue because the Sixth Circuit has not followed this Court's tradition of protecting medical privacy rights. *See U.S. Citizens Ass'n*, 705 F.3d at 601 (rejecting a "right to refuse unwanted medical care").

[2] The government's argument would support placing financial penalties on exercising the right to abortion. That would entail no mere loss of an "economic right," even though it is of a financial nature. Likewise here, Coons asserts a loss of a fundamental liberty.

Union Free School Dist., 395 U.S. 621, 627 (1969) (government must show law is narrowly tailored to achieve a compelling state interest). The government has not met this burden.

Because Coons has identified a protected liberty interest, ER70-71 ¶¶ 87-92, the district court erred in depriving him of the opportunity to introduce evidence substantiating his allegation that PPACA unduly burdens his right to medical autonomy.

II. Coons has a constitutional right to informational privacy and has stated a ripe claim that PPACA unduly burdens that right.

The government relies on *U.S. Citizens Ass'n* for the proposition that Coons can "avoid any privacy concern altogether by simply . . . complying with the individual mandate" and paying the tax. Response p. 11 (*quoting U.S. Citizens Ass'n*, 705 F.3d at 602).[3] But in any case presenting an "unconstitutional conditions" challenge, the government can claim that a plaintiff could avoid the concern by simply acquiescing in the burden imposed on his choice to exercise his

[3] Just as with the medical autonomy claim, *U.S. Citizens Ass'n* is inapposite because the Sixth Circuit does not protect privacy as comprehensively as this Court, nor does it recognize a general right to informational privacy. *Compare J.P. v. DeSanti*, 653 F.2d 1080, 1090-91 (6th Cir. 1981) ("not all rights of privacy or interests in nondisclosure of private information are of constitutional dimension, so as to require balancing government action against individual privacy") *with Tucson Woman's Clinic v. Eden*, 379 F.3d 531, 551 (9th Cir. 2004) (recognizing a "constitutionally protected interest in avoiding 'disclosure of personal matters,' including medical information," and applying a multi-factor balancing test). Thus, the Sixth Circuit's failure to even apply the balancing test to similar claims is inconsistent with this Court's jurisprudence.

rights. It is the being forced to confront that choice that is the gravamen of any unconstitutional conditions claim. *Koontz v. St. Johns River Water Mgmt. Dist.*, 133 S. Ct. 2586, 2594 (2013) (Constitution protects "rights by preventing the government from coercing people into giving them up"). What the government regards as merely a choice is in fact coercion, because the tax imposes an impermissible burden on the exercise of Coons' privacy right. Whether PPACA's requirement that Coons choose between handing over his private health information to third parties or paying a penalty constitutes an undue burden is a fact-driven inquiry. In dismissing the claim, the district court neither underwent the proper analysis nor made the necessary findings.

The government claims that the law contains safeguards sufficient to eliminate any injury, Response pp. 11-12, but these supposed protections neither mitigate Coons' concerns nor the Act's constitutional deficiencies. Assuming these alleged protections function properly, they would only prevent insurance companies from further disseminating Coons' information. *See* Response p. 12 ("Federal law places strict limits on the manner in which insurance companies may use or disclose individuals' medical information"). But Coons objects to being coerced into disclosing sensitive personal information *to any entity*, including the insurance companies that are clearly encompassed within the law's requirements. ER70-71 ¶¶ 88-92. But for PPACA, he would not be forced to choose between

yielding private information that he would otherwise keep confidential or paying a penalty. ER53-54 ¶¶ 14-16; ER55-56 ¶¶ 20-26.[4]

Moreover, once Coons discloses this information to an insurance company, it is subject to government appropriation. ER70-71 ¶¶ 88-92; *see* Opening Brief pp. 23-24 (citing cases and statutes). The Department of Health and Human Services (HHS) has announced that it plans to allow local, state, and federal governments to share the personal health information of those who seek insurance on the Act's health insurance exchanges. *Patient Protection and Affordable Care Act; Program Integrity: Exchange, SHOP, Premium Stabilization Programs, and Market Standards*, 78 Fed. Reg. 37,032 (Dep't of Health and Human Servs. June 19, 2013) (proposed rule), at 72-73 *available at* https://s3.amazonaws.com/public-inspection.federalregister.gov/2013-14540.pdf. And Michael Astrue, former HHS general counsel and Commissioner of the Social Security Administration, has revealed that the government's present system for collecting personal information in exchanges would "leave members of the public open to identity theft," would

[4] The government also understates the information insurers will solicit, emphasizing that PPACA "will bar most insurance plans from denying coverage or setting premiums on the basis of an individual's medical condition or history." Response p. 11. But this requirement provides an even *greater* incentive for insurance companies to solicit sensitive information from consumers. An insurance company's solvency depends on its ability assess risk and set premiums at an appropriate level, which would be nearly impossible without having any information about a customer's medical history. Coons will establish this through discovery.

result in "exposure of address for victims of domestic abuse and others," and would "inflict on the public the most widespread violation of the Privacy Act in our history." Michael Astrue, *Privacy Be Damned*, The Weekly Standard, August 5, 2013, *available at* http://www.weeklystandard.com/articles/privacy-be-damned_741033.html. HHS recently concluded that it "could not assess . . . efforts to identify security controls and systems risks for the [Health Insurance Exchange's Electronic] Hub and implement safeguards and controls to mitigate identified risks" and that it "could not assess . . . whether vulnerabilities identified by the testing would be mitigated." HHS Office of Inspector General, *Observations Noted During the OIG Review of CMS's Implementation of the Health Insurance Exchange – Data Services Hub*, August 2013, at 4-5 *available at* http://oig.hhs.gov/oas/reports/region1/181330070.pdf. Thus, by forcing Coons to decide between paying a penalty and relinquishing sensitive private information to third parties, the government is asking him to waive his Fourth Amendment expectation of privacy and subject himself to potential security threats.[5]

In any event, the alleged safeguards are among the factors that must be weighed against the privacy right at stake, which requires careful weighing of

[5] Under the voluntary relinquishment to private third parties doctrine, any information Coons discloses to an insurer can then be seized by the government without a warrant, ER70-71 ¶¶ 88-92, because the Supreme Court has held that individuals lack a reasonable expectation of privacy in information they "voluntarily" share by contracting with private companies. *United States v. Miller*, 425 U.S. 435, 443 (1976); *United States v. Jacobson*, 466 U.S. 109, 117 (1984).

evidence. *See Tucson Woman's Clinic*, 379 F.3d at 551 (listing factors). The government itself admits this, but advocates rejecting Coons' claim on 12(b)(6) grounds by citing to cases that turn on unique facts. Response pp. 12-14. *See, e.g.*, *Roe v. Sherry*, 91 F.3d 1270 (9th Cir. 1996) (considering privacy rights in the context of a search pursuant to a particular criminal investigation). Whether any factor "outweighs the individual's privacy interest . . . will necessarily vary from case to case." *Seaton v. Mayberg*, 610 F.3d 530, 538 (9th Cir. 2010), *cert. denied*, 131 S. Ct. 1534 (2011) (quotations and citations omitted). Moreover, several of the cases the government cites involved weighing privacy interests against a state's broad police powers, an entirely different assessment from that involved here. *See Whalen v. Roe*, 429 U.S. 589, 597-98 (1977) (emphasis added) (weighing privacy interests against "New York's *broad police power*" to "experiment[] with possible solutions to problems of *vital local concern*"); *Planned Parenthood of S. Ariz. v. Lawall*, 307 F.3d 783 (9th Cir. 2002) (emphasis added) (weighing privacy interests against *state's* interests).[6] Of course, Coons' claim is against the *federal* government, which "possesses only limited powers; the States and the people retain the remainder." *NFIB*, 132 S. Ct. at 2576. This difference alters the

[6] Another case involved weighing privacy interests against the federal government's interests as a *proprietor*, where the government "has a much freer hand." *NASA v. Nelson*, 131 S. Ct. 746, 757-59 (2011) (involving background checks for government employment conducted in the government's proprietary, not regulatory, capacity).

balancing test. To the extent that the government's cases are relevant, they illustrate the need to remand Coons' claim to the district court so that it can apply the balancing test to the unique circumstances of this case.

It is beyond question that PPACA forces Coons to either to disclose personal information to a third party insurance company – to which the government also has access – or pay an exaction for refusing to do so. That requirement conflicts with the right to informational privacy recognized by this Court. Thus the district court erred in dismissing Coons' well-pleaded privacy claim. The district court afforded Coons no opportunity to prove that the tax unduly burdens his rights, nor did it address any of the relevant factors discussed above. *See* ER6-9. The dismissal should be reversed.

III. Dr. Novack has stated a ripe claim that IPAB violates the separation-of-powers doctrine.

A. The district court did not fully and properly consider Novack's separation-of-powers claim

The government asks this Court to ignore the delegation portion of Novack's separation-of-powers claim because courts have upheld "seemingly vague principles." Response pp. 17-18 (*quoting In re National Sec. Agency Telecommunications Records Litigation*, 671 F.3d 881, 896 (9th Cir 2011), *cert. denied sub nom. Hepting v. AT&T Corp.*, 133 S. Ct. 421 (2012)). But the government's reliance on *In re National Sec. Agency* is misplaced because the law

in question in that case arose "within the realm of national security – a concern traditionally designated to the Executive as part of his Commander-in-Chief power," not to Congress as part of its legislative power. *Id.* at 897. In such cases, "the intelligible principle standard need not be overly rigid," *id.*, unlike in this case. That case did not involve a law that creates a permanent new regulatory body like PPACA does; that case addressed the circumstances under which the Attorney General can exercise his discretion to enforce a law. *Id.* at 896. And unlike IPAB, this exercise of discretion was subject to judicial review. *Id.* at 898. Here, the judiciary is statutorily excluded from reviewing whether IPAB is abiding by its vague directives or any other provision of the law.

The government insists that intelligible principles constrain IPAB, reciting numerous provisions supposedly guiding the Board. Response pp. 18-19. But the Act does not compensate in precision for what it lacks in brevity. These provisions are hopelessly vague and undefined, especially in light of IPAB's broad scope: the power to act "on matters related to the Medicare program." 42 U.S.C. § 1395kkk(c)(2)(A)(vi). For example, although the Act bars IPAB from "ration[ing] health care," §1395kkk(c)(2)(A)(ii), PPACA contains no definition of rationing care. Given that IPAB has power to take whatever action "related to the Medicare program," it is easily foreseeable that IPAB could take action that would qualify as "rationing." Yet because IPAB is immune from judicial review, any such action

would escape legal checks or balances. *See* Timothy Stoltzfus Jost, *The Real Constitutional Problem with the Affordable Care Act*, 36 J. Health Pol. Pol'y & L. 501, 504 (2011) ("IPAB could . . . dramatically reduc[e] payments for [medical services, which] might arguably violate the clause that enjoins the IPAB from establishing systems that ration care or restrict benefits, but these vague limitations certainly do not expressly prohibit such a proposal." This "decision would be immune from judicial review"). IPAB is the sole judge of whether it is obeying the law. *See* § 1395kkk(e)(5) (insulating IPAB from judicial and administrative review). *Cf. Amalgamated Meat Cutters & Butcher Workmen of N. Am., AFL-CIO v. Connally*, 337 F. Supp. 737, 746 (D.D.C. 1971) (emphasis added) (finding an intelligible principle because "compatibility with the legislative design may be ascertained not only by Congress *but by the courts and the public*").

The government cannot avoid a delegation problem simply by increasing a statute's word count. Instead, the proper assessment of whether Congress has unlawfully delegated the lawmaking power weighs the purported constraints on the delegate against the scope of power delegated. *See, e.g.*, *Whitman v. American Trucking Ass'ns*, 531 U.S. 457, 475 (2001) (degree of oversight necessary "varies according to the scope of the power congressionally conferred"); *Synar v. United States*, 626 F. Supp. 1374, 1386 (D.C. Cir. 1986) (emphasis in original), *aff'd sub nom. Bowsher v. Synar*, 478 U.S. 714 (1986) (constitutionality of delegation must

be judged "on the basis of its scope *plus* the specificity of the standards governing its exercise"). Neither defendants nor the district court employed such a balancing test.

In dismissing Plaintiffs' claim without engaging in *any* balancing or factual determinations, the district court failed to take into account the multiple factors that courts should consider when judging separation-of-powers claims. The government in its response commits the same error, considering and rejecting each factor in isolation. *See, e.g.*, Response p. 20 (courts "have upheld statutes against non-delegation challenges where judicial review was not available"); Response p. 23 ("there is no such constitutional requirement" that a board be bipartisan). But Novack does not contend that any one factor *on its own* is dispositive of whether PPACA violates the separation-of-powers doctrine. Instead, courts must "weigh[] a number of factors," *Commodities Futures Trading Comm'n v. Schor*, 478 U.S. 833, 851 (1986), and consider "the *aggregate effect* of the factors." *Synar*, 626 F. Supp. at 1390 (emphasis added). *See* Opening Brief pp. 36-38 (setting forth the relevant factors and corresponding tests courts apply in a separation-of-powers inquiry).[7]

[7] The government bizarrely contends that not all of the factors in Novack's separation-of-powers argument are properly before the Court. First, it claims that Novack cannot discuss the anti-repeal provisions, because he withdrew Count VI. Response pp. 20-21. But as Appellants acknowledged in their opening brief, they voluntarily dismissed the claim that IPAB's anti-repeal provisions *burden legislators' voting rights*, ER71-77 ¶¶ 93-114, due to the Supreme Court's governing decision in *Nevada Comm'n on Ethics v. Carrigan*, 131 S. Ct. 2343

Finally, the government contends that deciding Novack's separation-of-powers claim is unnecessary because the House and Senate can simply change their rules or Congress can repeal the entire Act, thus eliminating constitutional concerns. Response pp. 20-22. This approach provides no solace for Novack and ignores the purpose of separation of powers.[8] *See, e.g.*, *Loving v. United States*, 517 U.S. 748, 756 (1996) (citations omitted) ("Even before the birth of this country, separation of powers was known to be a defense against tyranny"); *Bond v. United States*, 131 S. Ct. 2355, 2365 (2011) ("The structural principles secured by the separation of powers protect the individual"). Permitting an otherwise unconstitutional law to stand simply because it was purportedly promulgated pursuant to Congress's rulemaking authority would effectively eradicate the Constitution's protections. Congress may not use its rulemaking authority to surmount constitutional restraints. *United States v. Smith*, 286 U.S. 6, 33 (1932).

PPACA's comprehensive consolidation of power in IPAB cries out for

---

(2011). Opening Brief p. 8 n.4. The anti-repeal provision is independently relevant to Novack's separation-of-powers claim, which remains viable. ER79 ¶ 123 ("The Act . . . purports to entrench the delegation of such powers against review by future Congresses"). Second, the government contends that other separation-of-powers arguments were not alleged in the complaint. Response p. 22. But these arguments are not independent claims at all; they are factors relevant to deciding the separation-of-powers claim.

[8]The government's contention that IPAB can police itself by volunteering to engage in notice-and-comment rulemaking even though the Act does not require it to do so, Response p. 23, is likewise unconvincing.

meaningful judicial scrutiny. Because the district court did not conduct a proper separation-of-powers analysis, its dismissal of Novack's claim should be reversed and remanded.

B. Novack has standing to challenge IPAB

Although the district court did not dismiss Novack's claim on standing grounds, ER12-13, the government claims that Novack lacks standing because his injuries are "speculative," Response p. 17, and "hypothetical." Response p. 15 (quoting *Hartman v. Summers*, 120 F.3d 157, 160 (9th Cir. 1997)). In *Hartman*, however, the plaintiff's injury was too speculative because he "failed to allege that he is subject to the release procedure that he complains of." 120 F.3d at 160. By contrast, Novack has alleged that he receives Medicare reimbursements and thus falls under IPAB's jurisdiction, ER51 ¶ 7, will suffer financial harm as a result of IPAB's actions, ER80 ¶ 128, and is injured by market displacements IPAB's existence has already set in motion. ER72-74 ¶¶ 99-102. Courts have found that plaintiffs subject to a governmental entity's authority have standing to challenge the creation of that entity. *See Nat'l Fed'n of Fed. Employees v. United States*, 727 F. Supp. 17, 21 (D.D.C. 1989), *aff'd*, 905 F.2d 400 (D.C. Cir. 1990) (plaintiff labor union organization had standing to challenge the Base Closure and Realignment Act under the separation of powers doctrine due to "the significant degree of

authority and control that the Department of Defense has over these civilian employees").

Novack also has standing because a plaintiff has standing to challenge the constitutionality of an agency whose primary directive is antithetical to the plaintiff's goals. In *Metropolitan Washington Airport Authority v. Citizens for Abatement of Aircraft Noise, Inc.*, 501 U.S. 252 (1991), a citizens' group concerned with the abatement of aircraft noise challenged the creation of a Board of Review empowered to veto the Airport Authority's decision to reduce air traffic at Washington National Airport. The Supreme Court held that the plaintiffs had standing to bring a separation-of-powers claim because:

> [T]he harm respondents have alleged is not confined to the consequences of a possible increase in the level of activity at National. The harm also includes the creation of an impediment to a reduction in that activity. . . . The Board of Review and the master plan, which even petitioners acknowledge is at a minimum "noise neutral," therefore injure [Plaintiffs] by making it more difficult for [Plaintiffs] to reduce noise and activity at National.

Id. at 265 (citations omitted). Just as the Board of Review "was created by Congress as a mechanism to preserve operations at National at their present level, or at a higher level if possible," *id.*, PPACA empowers IPAB to reduce – but not to increase – Medicare reimbursements in order to achieve a net reduction in total Medicare spending. ER80 ¶ 128. Just as the creation of the Board of Review "ma[de] it more difficult for [Plaintiffs] to reduce noise and activity" at the airport,

Metropolitan Washington Airport Auth., 501 U.S. at 265, IPAB's virtually unconstrained powers, combined with its directive to "reduce the per capita rate of growth in Medicare spending," 42 U.S.C. § 1395kkk(c), alters the procedure by which Novack is reimbursed for treating Medicare patients. ER51 ¶ 7; ER80 ¶ 128. *See also Synar*, 626 F. Supp. at 1381 (employee association had standing to bring a separation-of-powers challenge against a statute that automatically cut the national budget when the budget deficit exceeded a certain threshold because invalidating the law would preclude cancellation of financial benefits to group).

The Supreme Court's decision in *Bond v. United States* further bolsters Novack's standing to challenge IPAB. There the Court held that a plaintiff has "standing to object to [a law's] violation of a constitutional principle that allocates power within government." 131 S. Ct. at 2365. Individuals "are protected by the operations of separation of powers and checks and balances" so they may "rely[] on those principles in otherwise justiciable cases and controversies." *Id.* at 2365. Because IPAB lacks constitutionally required checks and balances, and subjects Novack to an unlawful procedure that threatens him with financial harm, ER51 ¶ 7; ER80 ¶ 128, Novack has standing to challenge its constitutionality.

This Court has held that a plaintiff "who is likely to suffer economic injury as a result of [governmental action] that changes market conditions satisfies [the injury] part of the standing test." *Barnum Timber Co. v. E.P.A.*, 633 F.3d 894, 901

(9th Cir. 2011) (citations omitted). *See also Clinton v. New York*, 524 U.S. 417, 432 (1998) (farmers' cooperative had standing to challenge Line Item Veto Act even though vetoed provision would not have directly benefitted the cooperative because the cancellation resulted in an unfavorable change in market conditions). In addition to the aforementioned allegations, Novack alleges that the mere anticipation of IPAB's operation is altering market conditions as doctors and patients prepare for the coming regulations. ER72-74 ¶¶ 99-102. Because this "Court routinely recognizes probable economic injury resulting from [governmental actions] that alter competitive conditions as sufficient to satisfy" the injury requirement, *Barnum Timber Co.*, 633 F.3d at 901, these allegations are sufficient to survive a motion to dismiss. *See Bates v. Mortgage Elec. Registration Sys., Inc.*, 694 F.3d 1076, 1080 (9th Cir. 2012).

The government argues that Novack's claim is not ripe because the President has not yet nominated any members to the Board. Response p. 16. But PPACA enables – indeed, *requires* – IPAB to operate even in the absence of voting members. In that case, it empowers the HHS Secretary to create and implement IPAB proposals. *See* 42 U.S.C. § 1395kkk(c)(5). The Secretary currently wields the Board's power, making Novack's claims ripe for review. The Court "will be in no better position later than [it is] now to confront the validity of" IPAB. *See Blanchette v. Connecticut General Ins. Corps.*, 419 U.S. 102, 145 (1974).

IV. The government and the decision below disregarded the Supreme Court's preemption jurisprudence.

Finally, the district court should not have dismissed Coons' claim that PPACA does not preempt Arizona's Health Care Freedom Act (HCFA). Ariz. Const. art. XXVII, § 2. In a few terse sentences, the government purports to answer Coons' thorough preemption analysis, declaring that if "Arizona law directly conflicts with Section 5000A . . . the state law is preempted by operation of the Supremacy Clause." Response p. 9.[9] But this conclusory assertion is squarely at odds with the Supreme Court's presumption "that the historic police powers of the States were not to be superseded by the Federal Act unless that was the clear and manifest purpose of Congress." *Wyeth v. Levine*, 555 U.S. 555, 565 (2009).

In *United States v. Windsor*, the Supreme Court recently reaffirmed the role of federalism in protecting rights in areas traditionally regulated by the states. *See* 133 S. Ct. 2675, 2690 (2013) (federal Defense of Marriage Act (DOMA) violates equal protection guaranteed by Fifth Amendment by interfering with definition and regulation of marriage that has historically been within the authority of the states). In striking down DOMA, the Court emphasized the Act had a "far greater reach" than the "discrete" and "limited federal laws that regulate the meaning of marriage

[9] Coons' claim is not that Arizona's HCFA preempts *federal* law, as the government insinuates, Response p. 9, but that HCFA is not preempted because federal law "does not clearly, directly and unequivocally override state laws or constitutional provisions, such as . . . the Health Care Freedom Act." ER81 ¶ 133.

in order to further federal policy." *Id.* Like PPACA, DOMA "enacts a directive applicable to [thousands of] federal statutes and . . . regulations. And its operation is directed to a class of persons that the laws of [several] States, have sought to protect." *Id.*

As Coons has previously noted, "preemption analysis does not justify a free-wheeling judicial inquiry into whether a state statute is in tension with federal objectives," but instead dictates that a "high threshold must be met if a state law is to be pre-empted for conflicting with the purposes of a federal Act" when the federal law regulates an area traditionally governed by states. *Chamber of Commerce of the United States v. Whiting*, 131 S. Ct. 1968, 1985 (2011). This is especially true when "Congress has legislated . . . in a field which the States have traditionally occupied," *Wyeth*, 555 U.S. at 565, such regulating the field of health care. *Id.* at 1195 n.3; *Medtronic Inc. v. Lohr*, 518 U.S. 470, 475 (1996); *Rush Prudential HMO, Inc.*, 536 U.S. 355, 387 (2002); *Gonzales v. Oregon*, 546 U.S. 243 (2006).

The government's response disregards this well-established preemption framework. Response p, 9. Because the district court likewise failed to perform this analysis, and because PPACA cannot meet the "high threshold" necessary to displace state law, the district court erred in dismissing Plaintiffs' non-preemption claim (Count VIII). ER3-5.

CONCLUSION

Because Appellants' claims of medical autonomy, privacy, separation-of-powers, and federalism are ripe and worthy of judicial deliberation, Coons and Novack should be afforded the opportunity to prove their claims. Accordingly, they respectfully request that this Court reverse the decision below and remand for adjudication on the merits.

Respectfully Submitted,

/s/ Christina Sandefur
Clint Bolick
Kurt Altman
Nicholas C. Dranias
Christina Sandefur
Goldwater Institute
Scharf-Norton Ctr. for Const. Lit.
500 East Coronado Road, Phoenix, AZ 85004
(602) 462-5000
facsimile: (602) 256-7045
cbolick@goldwaterinstitute.org
kaltman@goldwaterinstitute.org
ndranias@goldwaterinstitute.org
csandefur@goldwaterinstitute.org

CERTIFICATE OF COMPLIANCE

I certify that this brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief is 4,541 words, excluding the portions exempted by Fed. R. App. P. 32(a)(7)(B)(iii). I further certify that this brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2013 and Times New Roman 14 point font.

/s/ Christina Sandefur

CERTIFICATE OF SERVICE

The attached filing has been electronically filed and served by ECF upon the persons identified in the below Service List.

/s/ Christina Sandefur

SERVICE LIST

Alisa Beth Klein
Mark B. Stern
Dana Kaersvang
DOJ - U.S. Department of Justice
Civil Division - Appellate Staff
950 Pennsylvania Avenue, N.W.
Washington, DC 20530
alisa.klein@usdoj.gov
mark.stern@usdoj.gov
Attorneys for Appellees Jacob J. Lew, Kathleen Sebelius, Eric Holder, Jr., and Barack Hussein Obama

Case No. 13-15324

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

NICK COONS and ERIC NOVACK;
Plaintiffs-Appellants,

vs.

JACOB J. LEW (in his official capacity as Secretary of the United States Department of the Treasury); KATHLEEN SEBELIUS (in her official capacity as Secretary of the United States Department of Health and Human Services); ERIC HOLDER, JR. (in his official capacity as Attorney General of the United States); and BARACK HUSSEIN OBAMA (in his official capacity as President of the United States);
Defendants-Appellees.

APPELLANTS' SUPPLEMENTAL APPENDIX (REPLY BRIEF)

Appeal from the United States District Court for the State of Arizona
Case No. 2:10-CV-1714-GMS, Hon. Murray Snow, presiding

Date Submitted: August 14, 2013

Clint Bolick
Kurt Altman
Nicholas C. Dranias
Christina Sandefur
GOLDWATER INSTITUTE
Scharf-Norton Ctr. for Const. Lit.
500 E. Coronado Rd.
Phoenix, AZ 85004
P: (602) 462-5000/F: (602) 256-7045

cbolick@goldwaterinstitute.org
kaltman@goldwaterinstitute.org
ndranias@goldwaterinstitute.org
csandefur@goldwaterinstitute.org
Attorneys for Appellants

TABLE OF CONTENTS

DEPARTMENT OF HEALTH AND HUMAN SERVICES

45 CFR Parts 144, 147, 153, 155, and 156

[CMS-9957-P]

RIN 0938-AR82

Patient Protection and Affordable Care Act; Program Integrity: Exchange, SHOP, Premium Stabilization Programs, and Market Standards

AGENCY: Centers for Medicare & Medicaid Services (CMS), HHS.

ACTION: Proposed rule.

SUMMARY: This proposed rule sets forth financial integrity and oversight standards with respect to Affordable Insurance Exchanges; Qualified Health Plan (QHP) issuers in Federally-facilitated Exchanges (FFEs); and States with regard to the operation of risk adjustment and reinsurance programs. It also proposes additional standards with respect to agents and brokers. These standards, which include financial integrity provisions and protections against fraud and abuse, are consistent with Title I of the Patient Protection and Affordable Care Act as amended by the Health Care and Education Reconciliation Act of 2010, referred to collectively as the Affordable Care Act.

DATES: To be assured consideration, comments must be received at one of the addresses provided below, no later than 5 p.m. on **[**OFR--insert date 30 days after date of publication in the **Federal Register]**.

ADDRESSES: In commenting, please refer to file code CMS-9957-P. Because of staff and resource limitations, we cannot accept comments by facsimile (FAX) transmission.

You may submit comments in one of four ways (please choose only one of the ways listed):

necessary information. Accordingly, we anticipate that this paragraph will be implicated most frequently with respect to paper applications. We seek comment on this proposal, including whether Exchange flexibility is appropriate; whether 15 days and 90 days are the right lower and upper limits; and whether additional language is needed to ensure coordination between the Exchange, Medicaid, and CHIP.

b. Verification of eligibility for minimum essential coverage other than through an eligible employer-sponsored plan (§155.320)

As finalized in the Exchange Establishment Rule, §155.320(b) specifies standards related to the verification of eligibility for minimum essential coverage other than through an eligible employer-sponsored plan. We propose to redesignate paragraph (b)(1) as (b)(1)(i) and (b)(2) as (b)(1)(ii) to consolidate the standards for Exchange responsibilities in connection with verification of eligibility for minimum essential coverage other than through an eligible employer-sponsored plan. In paragraph (b)(1)(i), we also propose to add the phrase "for verification purposes" to the end of existing text. This would clarify that HHS would provide a response to the Exchange to verify the information transmitted from the Exchange to HHS about an applicant's eligibility for or enrollment in minimum essential coverage other than through an eligible employer sponsored plan, Medicaid, CHIP, or the Basic Health Program. The Exchange would submit specific identifying information to HHS and HHS would verify applicant information with information from the Federal and State agencies or programs that provide eligibility and enrollment information regarding minimum essential coverage. Such agencies or programs may include but are not limited to Veterans Health Administration, TRICARE, and Medicare. HHS will work with the appropriate Federal and State agencies to complete the appropriate computer matching agreements, data use agreements, and information exchange

agreements which will comply with all appropriate Federal privacy and security laws and regulations. The information obtained from Federal and State agencies will be used and redisclosed by HHS as part of the eligibility determination and information verification process set forth in subpart D of part 155.

In connection with the proposal to redesignate paragraph (b)(2) to paragraph (b)(1)(ii), we are not proposing any change to the text of the provision as previously finalized. Consistent with the authorizations for the disclosure of certain information under 42 CFR 435.945(c) and 457.300(c), this regulation provides for an Exchange to verify whether an applicant has already been determined eligible for coverage through Medicaid, CHIP, or the Basic Health Program, using information obtained from the agencies administering such programs.

Finally, we propose to add paragraph (b)(2) to provide that consistent with 45 CFR 164.512(k)(6)(i) and 45 CFR 155.270, a health plan that is a government program providing public benefits, is expressly authorized to disclose PHI, as that term is defined at 45 CFR 160.103, that relates to eligibility for or enrollment in the health plan to HHS for verification of applicant eligibility for minimum essential coverage as part of the eligibility determination process for advance payments of the premium tax credit or cost-sharing reductions. We intend for this provision to enable any health plan that is a government program within the scope of 45 CFR 164.512(k)(6)(i) to disclose the protected health information necessary for HHS to be able to verify of minimum essential coverage as required to conduct eligibility determinations for insurance affordability programs. We seek comment on this proposal.

c. Administration of Advance Payments of the Premium Tax Credit and Cost-Sharing Reductions (§155.340)

Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

OBSERVATIONS NOTED DURING THE OIG REVIEW OF CMS'S IMPLEMENTATION OF THE HEALTH INSURANCE EXCHANGE—DATA SERVICES HUB

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Gloria L. Jarmon
Deputy Inspector General

August 2013
A-18-13-30070

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.

DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL
WASHINGTON, DC 20201

August 2, 2013

TO: Marilyn Tavenner
Administrator
Centers for Medicare & Medicaid Services

Tony Trenkle
Chief Information Officer
Centers for Medicare & Medicaid Services

FROM: /Gloria L. Jarmon/
Deputy Inspector General for Audit Services

SUBJECT: Memorandum Report: Observations Noted During the OIG Review of CMS's Implementation of the Health Insurance Exchange—Data Services Hub (A-18-13-30070)

This memorandum report provides the results of our review of the Centers for Medicare & Medicaid Services' (CMS) implementation of the Data Services Hub (Hub) from a security perspective. To determine the status of the implementation of the Hub, we assessed the information technology (IT) security controls that CMS is implementing for the Hub, adequacy of the testing activities being performed during its development, and the coordination between CMS and Federal and State agencies during the development of the Hub. A memorandum report is the best vehicle to communicate the results of our performance audit work when observations, not recommendations, are the key elements of our results.

SUMMARY

CMS is addressing and testing security controls of the Hub during the development process. However, several critical tasks remain to be completed in a short period of time, such as the final independent testing of the Hub's security controls, remediating security vulnerabilities identified during testing, and obtaining the security authorization decision for the Hub before opening the exchanges. CMS's current schedule is to complete all of its tasks by October 1, 2013, in time for the expected initial open enrollment period.

BACKGROUND

States must establish health insurance exchanges by January 1, 2014,[1] and all health insurance exchanges must provide an initial open enrollment period beginning October 1, 2013 (45 CFR § 155.410). Health insurance exchanges are State-based competitive marketplaces where individuals and small businesses will be able to purchase private health insurance. Exchanges will serve as a one-stop shop where individuals will get information about their health insurance options, be assessed for eligibility (for, among other things, qualified health plans, premium tax credits, and cost sharing reductions), and enroll in the health plan of their choice. A State may elect to operate its own State-based exchange or partner with the Federal Government to operate a State partnership exchange. If a State elects not to operate an exchange, the Department of Health and Human Services will operate a Federally Facilitated Exchange.[2] For the purposes of this report, "exchanges" refers to all three types of health insurance exchanges.

The Hub is intended to support the exchanges by providing a single point where exchanges may access data from different sources, primarily Federal agencies. It is important to note that the Hub does not store data. Rather it acts as a conduit for exchanges to access the data from where they are originally stored. The functions of the Hub will include facilitating the access of data by exchanges; enabling verification of coverage eligibility; providing a central point for the Internal Revenue Service (IRS) when it asks for coverage information; providing data for oversight of the exchanges; providing data for paying insurers; and providing data for use in Web portals for consumers.

Effective security controls are necessary to protect the confidentiality, integrity, and availability of a system and its information. The National Institute of Standards and Technology (NIST) developed information security standards and guidelines, including minimum requirements for Federal information systems. CMS is required to follow the NIST security standards and guidelines in securing the Hub.[3]

OBJECTIVE, SCOPE, AND METHODOLOGY

Our primary audit objective was to determine CMS's current progress in implementing security requirements for the Hub. We evaluated the adequacy of the development and testing of the Hub from a security perspective. We did not review the functionality of the Hub.

---

[1] The Patient Protection and Affordable Care Act § 1311(b) (P.L. No. 111-148) and the Health Care Reconciliation Act of 2010 (P.L. No. 111-152), collectively known as the Affordable Care Act (ACA).

[2] The Center for Consumer Information and Insurance Oversight Web site has further information on the health insurance exchanges: http://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces. Accessed on July 9, 2013.

[3] NIST's security standards assist Federal agencies in implementing the requirements under the Federal Information Security Management Act of 2002, 44 U.S.C. §§ 3541, *et seq*.

To accomplish our objectives, we:

- reviewed documentation, System Development Life Cycle artifacts, and CMS project schedules and timelines (including milestones established by CMS) as of March and May 2013 (the dates of CMS's two project schedules) to track the activities that need to be completed before the implementation of the Hub;
- interviewed CMS employees and contractors;
- interviewed personnel from key Federal agencies working with CMS during the development of the Hub; and
- reviewed CMS's security testing results.

We performed our fieldwork substantially from March through May 2013.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

RESULTS

At the time of our review, CMS and its contractors were continuing to develop the Hub and work with its Federal and State partners in testing the Hub to ensure its readiness in time for the initial open enrollment to begin on October 1, 2013. We made the following observations on security controls, security testing, and coordination at the time of our fieldwork.

Assessment of Security Controls

According to NIST security standards, every Federal information system must obtain a security authorization before the system goes into production. The security authorization is obtained from a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations.

The security authorization package must include a system security plan (SSP), information security risk assessment (RA), and security control assessment (SCA) report. The security authorization package provides important information about risks of the information system, security controls necessary to mitigate those risks, and results of security control testing to ensure that the risks have been properly mitigated. Therefore, these documents must be completed before the security authorization decision can be made by the authorizing official. The authorizing official may grant the security authorization with the knowledge that there are still risks that have not been fully addressed at the time of the authorization.

CMS incorporated the elements required for adequate security into the draft Hub SSP. The SSP provides an overview of the security requirements of the system and describes the controls in place or planned (e.g., access controls, identification and authentication) for meeting those requirements and delineates the responsibilities and behavior expected of all individuals who access the system. The information security Hub RA was being drafted during our fieldwork. The RA should identify risks to the operations (including mission, functions, image, or reputation), agency assets, and individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. However, the CMS contractor did not expect to provide finalized security documents, including the SSP and RA, to CMS for its review until July 15, 2013. The original dates listed in CMS's March and May 2013 schedules for the contractor to submit the final security documents were May 6, 2013, and July 1, 2013, respectively. Because the documents were still drafts, we could not assess CMS's efforts to identify security controls and system risks for the Hub and implement safeguards and controls to mitigate identified risks.

According to CMS's current timeline, the security authorization decision by the authorizing official, the CMS Chief Information Officer (CIO), is expected on September 30, 2013; the March 2013 schedule reported the date as September 4, 2013. If there are additional delays in completing the security authorization package, the CMS CIO may not have a full assessment of system risks and security controls needed for the security authorization decision by the initial opening enrollment period expected to begin on October 1, 2013.

Adequacy of Security Testing

CMS and its contractors are performing security testing throughout the Hub's development, including vulnerability assessments of Hub services. CMS is logging and tracking defects and vulnerabilities throughout the development process and correcting and retesting Hub services to ensure that vulnerabilities are remediated.

An SCA of the Hub must be performed by an independent testing organization before the security authorization is granted.[4] The SCA determines the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome of meeting the security requirements for the information system. The goal of the SCA test plan is to explain clearly the information the testing organization expects to obtain prior to the SCA, the areas that will be examined, and the proposed scheduled activities expected to be performed during the SCA. According to CMS's March 2013 schedule, the SCA test plan was scheduled to be provided to CMS for its review on May 13, 2013, and the SCA was scheduled to be performed between June 3 and 7, 2013. However, in the May 2013 schedule, the SCA test plan due date was moved to July 15, 2013, and the SCA is now scheduled to be performed between August 5 and 16, 2013. CMS stated that the SCA was moved so that performance stress testing of the Hub could be finished before the SCA and any vulnerabilities identified during the stress

[4] NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, Revision 1.

testing could be remediated. Otherwise, CMS might need to perform an additional SCA after the remediation was complete.

CMS has 3 weeks between the receipt of the SCA test plan and the start of the SCA for CMS to make changes to the plan and for the independent testing organization to adjust the plan. CMS must ensure that all devices in the Hub environment, including all firewalls and servers, are analyzed during the SCA. In addition, the draft report with the results of the SCA is not due from the contractor performing the SCA until September 9, 2013, and the final report is not due until September 20, 2013. We could not assess planned testing or whether vulnerabilities identified by the testing would be mitigated because the SCA test plan had not been provided and the SCA had not been completed at the time of our review. If there are additional delays in completing the SCA test plan and performing the SCA, the authorizing official may not have the full assessment of implemented security controls needed for the security authorization decision by the initial opening enrollment period expected to begin on October 1, 2013.

See the table for a summary of the key security dates.

Table: Key Hub Security Due Dates

Security Document	Date Due (per March 2013 schedule)	Date Due (per May 2013 schedule)
Final SSP and RA	May 6, 2013	July 1, 2013*
SCA Test Plan	May 13, 2013	July 15, 2013
SCA	June 3-7, 2013	August 5-16, 2013
Draft SCA Report	June 28, 2013	September 9, 2013
Final SCA Report	July 15, 2013	September 20, 2013
Security Authorization Decision	September 4, 2013	September 30, 2013

* On July 1, 2013, CMS stated that the new date for the SSP and RA is July 15, 2013.

Coordination Among CMS and Its Federal and State Partners

CMS is coordinating with its Federal and State partners during the development and testing of the Hub, in part to ensure that security measures are implemented by all stakeholders. The Federal partners are the IRS, Social Security Administration (SSA), Department of Homeland Security (DHS), Veterans Health Administration (VHA), Department of Defense (DOD), Office of Personnel Management (OPM), and Peace Corps.

CMS developed a testing approach for interagency testing and has developed test plans. CMS is in the process of executing its test plans, which include testing for secure communications between CMS and its Federal and State partners and performance stress testing of the Hub.

CMS also developed security-related documents related to the Hub and the exchanges. CMS developed Interface Control Documents (ICD) with all of its Federal partners. The ICDs should be established during the development of new systems. The ICDs provide a common, standard technical specification for transferring ACA-related information between CMS (the Hub) and its Federal partners. The ICDs establish standard rules, requirements, and policies (including security-related policies) with which the development and implementation of the interfaces between CMS and its Federal partner must comply. CMS and its Federal partners collaborated in the development of the ICDs and signed the ICDs in May 2013.

Federal policy requires agencies to develop Interconnection Security Agreements (ISA) for Federal information systems and networks that share or exchange information with external information systems and networks. Specifically, Office of Management and Budget Circular A-130, Appendix III, requires agencies to obtain written management authorization before connecting their IT systems to other systems. The written authorization should define the rules of behavior and controls that must be maintained for the system interconnection. The Master ISA describes the systems' environment, network architecture, and the overall approach for safeguarding the confidentiality, integrity, and availability of shared data and system interfaces. In addition, the Master ISA contains information on CMS information security policy and the roles and responsibilities pertaining to the maintenance of the security of ACA systems.

CMS completed a preliminary review of the Master ISA between CMS and the developer of the Hub on April 2, 2013, and the Associate ISAs on May 15, 2013. Each of the Federal partners will provide similar information pertaining to the partner agency in the Associate ISAs and signed by the Federal partner authorized official. The final review of the ISAs for all Federal partners is scheduled to be completed by September 3, 2013 and the CMS CIO is scheduled to grant the authority to connect to the Hub by September 30, 2013. In addition, CMS has developed a non-Federal ISA for third parties and the States.

A service level agreement (SLA) is a negotiated agreement between a service provider and the customer that defines services, priorities, responsibilities, guarantees, and warranties by specifying levels of availability, serviceability, performance, operation, or other service attributes. A SLA is needed between CMS and each of its Federal partners to establish agreed-upon services and availability, including response time and days and hours of availability of the Hub and the Federal partner's ACA systems. According to CMS's project schedule, the SLA with IRS was completed on March 15, 2013; the SLA with DHS is expected to be signed by July 26, 2013; and the SLA with SSA is expected to be signed by September 27, 2013. The SLAs with the remaining Federal partners (VHA, DOD, OPM, Peace Corps) are expected to be signed by September 20, 2013. The SLAs should be approved by all parties before October 1, 2013.

SUMMARY OF OBSERVATIONS

This memorandum report informs stakeholders of the status of steps CMS is taking to ensure that there are adequate security measures for the Hub. CMS is working with very tight deadlines to ensure that security measures for the Hub are assessed, tested, and implemented by the expected

initial open enrollment date of October 1, 2013. If there are additional delays in completing the security assessment and testing, the CMS CIO may have limited information on the security risks and controls when granting the security authorization of the Hub.

CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS

In its comments on our draft report, CMS stated that it is confident that the Hub will be operationally secure and it will have a security authorization before October 1, 2013. CMS also provided technical comments, which we addressed as appropriate. We have included CMS's comments in the Appendix.

APPENDIX: CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

Administrator
Washington, DC 20201

DATE: JUL 31 2013

TO: Kay L. Daly
Assistant Inspector General

FROM: Marilyn Tavenner
Administrator

SUBJECT: Office of Inspector General (OIG) Draft Report: "Observations Noted During the OIG Review of CMS's Implementation of the Health Insurance Exchange – Data Services Hub" (A-18-13-30070)

Thank you for providing the Centers for Medicare & Medicaid Services (CMS) with the opportunity to comment on the above subject OIG Draft report.

The CMS greatly appreciates the work of OIG in reviewing our program. CMS leadership is closely monitoring the critical task of conducting independent security testing and managers are adept at scheduling and performing testing on all new systems in accordance with an established development life-cycle process. In regards to the Hub, independent test dates have been adjusted to align precisely with each code delivery date. As OIG noted in this report, to mitigate this concern CMS is conducting internal security testing reviews and fixing system weaknesses as part of the development process. This approach has proven to significantly reduce security weaknesses discovered by an independent auditor. CMS has prioritized review of the audit reports and is confident the Hub will be operationally secure and it will have an authority to operate prior to Oct 1, 2013.

The CMS thanks OIG for the work done on this issue and looks forward to working with OIG in the future.

Office of Inspector General Note—Technical comments in the auditee's response to the draft have been omitted from the final report and all appropriate changes have been made.

the weekly Standard
www.weeklystandard.com

Published on *The Weekly Standard* (http://www.weeklystandard.com)

Privacy Be Damned

The imminent health-exchange scandal.

Michael Astrue

August 5, 2013, Vol. 18, No. 44

I have been dismayed, but unsurprised, to see that the Department of Health and Human Services (HHS) is already spinning the launch of its federal health insurance exchange this October. The federal and state "exchanges" — HHS recently rebranded them "marketplaces" — are a linchpin of the Affordable Care Act (ACA) that would allow uninsured Americans to assess and select health insurance plans. Repeated HHS assurances that the systems will be ready for launch have been a critical factor in state decisions as to whether they should use the HHS portal or build their own; at least 14 states have wisely chosen to build their own systems.

A functional and legally compliant federal exchange almost certainly will not be ready on October 1 for those who will have no choice but to use the federal portal. The reasons for failure are not short timelines (Congress gave HHS more than three years), political interference (Congress has not focused on ACA systems), or complexity (states have built well-designed exchanges). The reason is plain old incompetence and arrogance.

After enactment of the ACA, the former administrator of the Centers for Medicare and Medicaid Services (CMS), Donald Berwick, had the responsibility of creating systems for the exchanges, which required peripheral support from the Social Security Administration (SSA) and the Internal Revenue Service (IRS). Congress did not appropriate special funding for this initiative, and Berwick was unwilling to shift adequate funds within CMS for this critical project. Berwick then failed to persuade HHS secretary Kathleen Sebelius to spend one penny on this effort from her massive ACA discretionary fund. Berwick also failed to bully SSA into paying for the entire system; he brushed aside the blatant illegality of that approach.

Civil servants at CMS did what they could to meet the statutory deadline — they threw together an overly simplistic system without adequate privacy safeguards. The system's lack of any substantial verification of the user would leave members of the public open to identity theft, lost periods of health insurance coverage, and exposure of address for victims of domestic abuse and others. CMS then tried to deflect attention from its shortcomings by falsely asserting that it had done so to satisfy White House directives about making electronic services user-friendly.

In reality, the beta version jammed through a few months ago will, unless delayed and fixed, inflict on the public the most widespread violation of the Privacy Act in our history. Almost a year ago both I and the IRS commissioner raised strong legal objections to the Office of Management and Budget (OMB), which has statutory oversight responsibilities for the Privacy Act. As of the time of my resignation as commissioner of Social Security last February, OMB lawyers could not bring themselves to bless a portal in which I could change Donald Trump's health insurance and he could change mine.

Incredibly, at the time of our appeal, no senior legal official at HHS had reviewed the legal issues raised by this feature of the ACA. It is my understanding that OMB, despite the recent furor over this administration's lack of respect for the privacy of citizens, has ordered agencies to bulldoze through the Privacy Act by invoking an absurdly broad interpretation of the Privacy Act's "routine use" exemption.

The Privacy Act is a general prohibition, subject to narrow exceptions, on disclosure of records between agencies or to the public. The "routine use" exception allows disclosure when the use of a record is "for a purpose which is compatible with the purpose for which it is collected." Privacy being essential to patient care, it is impossible to justify a "routine use" exception for a system knowingly built in a way that will permit disclosure of intimate health care data.

In this regard, the administration is not only preparing to violate the law, it is also holding itself to a far lower privacy standard than that to which it is trying to hold the private sector. In announcing the administration's "Consumer Privacy Bill of Rights," last year President Obama himself said, "American consumers can't wait any longer for clear rules of the road that ensure their personal information is safe online."

A June Government Accountability Office (GAO) report gingerly avoided all the significant privacy and operational issues surrounding the HHS system, and did little more than report that CMS admitted it was behind on certain parts of the program but felt it could catch up. Nowhere did our congressional watchdogs show any sign that they had actually tested the system and considered its readiness for public use.

Since the HHS inspector general and GAO have been snoozing on their watches, it is time for Congress itself to inspect the current version of the HHS software and decide whether delay of implementation of the exchanges is the right course of action.

Michael Astrue served as HHS general counsel (1989-1992) and commissioner of Social Security (2007-2013).
