March 30, 2001

Honorable Tommy G. Thompson
Secretary of Health & Human Services
Washington, D.C. 20201

RE: HHS Final Rule on Standards for Privacy of Individually Identifiable Health Information; 65 Fed. Reg. 82462 (December 28, 2000)

Dear Secretary Thompson:

The Office of Advocacy of the U.S. Small Business Administration (SBA) was established by Congress pursuant to Pub. L. No. 94-305 to advocate the views of small business before federal agencies and Congress. Advocacy is required by section 612(a) of the Regulatory Flexibility Act (RFA)[1] to monitor agency compliance with the RFA. In addition, the Chief Counsel of Advocacy is authorized to appear as *amicus curiae* in regulatory appeals from final agency actions, and is allowed to present views with respect to compliance with the RFA, the adequacy of the rulemaking record with respect to small entities, and the effect of the rule on small entities.[2] On March 28, 1996, the Small Business Regulatory Enforcement Fairness Act (SBREFA)[3] was signed into law making a number of significant changes to the RFA, including the provision to allow judicial review of agencies' compliance with the RFA.[4]

The Office of Advocacy has been involved at every stage of the privacy regulation—attending meetings with high-level HHS and OMB staff, and submitting comments on the various drafts of the regulation. Throughout this process, Advocacy has consistently urged HHS to pay closer attention to the burden associated with small business compliance. Although the final regulation reflected substantial changes and improvements over the proposed rule, the administrative burden associated with compliance still falls disproportionately to small businesses. This result seems ironic in that one of the intended statutory goals of the regulation was supposed to be administrative simplification.[5]

According to the cost estimates provided in the rule, small offices and clinics of doctors of medicine along with small offices and clinics of dentists will bear 47.5% (nearly $917

[1] 5 U.S.C. § 601 et seq.
[2] *Id.*
[3] Pub. L. No. 104-121, 110 Stat. 857 (1996).
[4] 5 U.SC. § 611.
[5] The privacy regulation is the second final rule to emerge as part of a package of Health Insurance Portability and Accountability Act (HIPAA) administrative simplification rules. The first rule dealt with standards for electronic transactions (see 65 Fed. Reg. 50312, August 17, 2000).

million) of the total cost of the regulation in the first year, and 49% (nearly $5.6 billion) of the total costs over ten years.[6] One can argue that there are more physician and dentist offices than other types of providers, but one cannot ignore the fundamental economic principle that the smallest businesses—usually the physicians and dentists—bear a higher burden in proportion to their revenues. It is for this reason that Advocacy proposed alternatives to reduce the burden on these providers during the draft phases of the rule.

Initially, during the draft proposal stage, Advocacy had hoped that small businesses would be given the choice to opt out of the rule's provisions in favor of an all-consent based system. That is, rather than appoint a privacy official, train all employees that handle confidential patient documents, create business associate contracts, keep detailed records, figure out the minimum necessary information requirements, etc.; a small business would instead need to obtain a signed consent for most instances where identifiable individual health information is shared with a third party. While this alternative may have generated more paperwork, it seemed to be simpler, and thus, may have contributed to greater compliance among providers and greater privacy for patients.

The second alternative arose during the draft final stage. Advocacy, realizing that HHS fully intended to maintain its overall scheme of imposing the same requirements on businesses of all sizes, urged the agency to publish sample forms, contracts and compliance plans prior to the rule's implementation date. The intent behind this alternative was to minimize the start-up costs of compliance. Rather than hiring lawyers or paying outside consultants to create business associate contracts, or figure out the appropriate disclosure requirements,[7] etc., a small business could use sample documents provided by the agency. This option would not have removed any flexibility from the rule, and it would have allowed businesses a place from which to start.

The rule does pledge to provide some sample forms (e.g., consent agreements), and to work with industry and trade groups to create these forms and guides, but there does not appear to be a commitment to complete the task prior to the rule's implementation. In addition, the partnership between HHS and the trade groups to publish these documents does not assure that there will be no cost to practitioners. Advocacy believes that HHS should publish these documents and make them available on the agency's website.

Advocacy urges the agency to use this time of temporary delay to reassess the burden placed on small businesses. According to the American Medical Association, there are over 110,000 pages of Medicare rules, policies and regulations for Medicare-participating

[6] 65 Fed. Reg. at 82788 (December 28, 2000).

[7] In the final rule, there are different use and disclosure requirements for: facility directory information, family members or personal representatives, public health officials, domestic violence cases, health oversight activities, judicial and administrative proceedings, law enforcement, decedents, organ donation and transplantation, research purposes, averting imminent threat to health or safety, specialized government functions (e.g., military, intelligence and correctional facilities), and disclosures to comply with worker's compensation laws.

physicians, and a high percentage of physicians report spending 20%-50% of their time on paperwork requirements. These are just Medicare regulations! A 1995 report published by Advocacy used conservative estimates to find that the cost of regulatory compliance for a large business (>500 employees) per employee was $3,400, and $5000 for small firms (< 500 employees).[8] This means that small businesses pay at least 30% more per employee to comply with regulations. The percentage goes up dramatically when the number of employees drops. The time is fast approaching when the time and cost spent on regulatory compliance will exceed the time spent on patient care and vital continuing medical education.

HHS announced on March 27, 2001 that it intends to simplify the medical privacy regulation and take steps to lessen the financial burden the rule has on providers. These changes will be announced in about 30 days. In the meantime, Advocacy would like to present some of its concerns regarding certain provisions of the final rule.

1. In spite of the rule's cost and complexity, patient privacy is still not assured. Personal health information will still be available to various entities for purposes not related to treatment or billing. For instance, much of the impetus for patient privacy legislation came about because of complaints that drug companies and others were marketing commercial products and services based on patient/customer lists purchased from others (e.g., chain pharmacies) without the patient's permission. Under the final rule, this is still allowed, but a patient has the right to request that marketing solicitations stop after the first instance—in which case, the damage has already been done. Also, a patient can request restrictions on certain disclosures—assuming a patient thinks to ask for such a restriction at the outset of care—but providers do not have to accept such requests. It is bizarre that small businesses will pay $11.2 billion over the next ten years in order to comply with this patient privacy regulation, yet patients' names can still be sold to marketers for no legitimate health care purpose.

   In addition, entities that have the potential to violate patient privacy, like marketers, law enforcement, etc. (i.e., those that are not business associates or covered entities), are not covered by the privacy rules. This is a fatal flaw of the authorizing statute, but the point is that billions are being spent, by small businesses in particular, and patient privacy is not assured.

2. HHS stretched its authority in order to regulate indirectly "business associates"—a type of entity not contemplated in the authorizing statute. While the final rule appears to impose less burden than the proposed rule, Advocacy believes that HHS has underestimated the impact of this provision. In the proposed rule, physicians and other covered entities would be held responsible for privacy violations of their business associates. Moreover, there was an active duty to monitor or "ensure"

[8] SBA Office of Advocacy, *The Changing Burden of Regulation, Paperwork and Tax Compliance on Small Business—A Report to Congress* (October 1995).

compliance of business associates. The final rule imposes sanctions on covered entities only if there was a known violation of the business associate contract, but also requires the covered entity to mitigate any known harmful effects of a business associate's violation. In practice, this new requirement to mitigate may have the same impact as the duty to ensure compliance. Fearful of potential negligence claims, or desiring to avoid unknown mitigation costs, covered entities may not be able to avoid actively monitoring their business associates.

3. The agency's authority to regulate business partners (albeit indirectly) and include all types of records (electronic and written records) remains unclear. These two provisions vastly increase the scope of the regulation. Moreover, in discussing records, HHS indicated in the proposed rule that extending the rule's scope beyond electronic records was "inconsistent with the intent of HIPAA provisions." Even though extending the scope of the rule to all records eliminates the confusion of having to deal separately with written and electronic records, it is important to state the legal authority for the agency's policy reversal. The agency should seek clarifying legislation from Congress before treading into these legally murky areas in order to protect itself from litigation and to avoid unnecessary burden to providers.

4. At the outset of its discussion of costs, the agency states that they "consistently made conservative assumptions . . . that, if incorrect are more likely to overstate rather than understate the true cost."[9] In reviewing the rule, however, it is difficult to see how the assumptions can be called conservative—particularly since the agency does not explain the basis for most of its assumptions. The assumptions are highly relevant because they form the basis of the cost estimates. If the assumptions are too low, then the cost of the regulation could be substantially higher. Note the following examples where the costs are not fully explained or seem exceptionally low:

- The agency assumes that the designated privacy official in a non-hospital setting will have to spend 26 hours per year complying with the regulation, and hospitals and health plans will spend 156 hours per year.[10]
- The agency also assumes that a complaint will be filed for one in every thousand patients, and that it will take 10 minutes for the privacy official or other employee to record the complaint.[11]
- The agency assumes that 90% of providers already use consent forms and that there will be a nominal cost of $0.05 per form for changing the language of the consent forms to comport with the regulation. The agency also assumes the same cost for creating entirely new consent forms for the 10% that do not already use the forms. The total first year cost for this activity is $166.[12]

[9] 65 Fed. Reg. at 82760.
[10] *Id.* at 82768.
[11] *Id.*
[12] *Id.* at 82771.

- The agency assumes that only 5% of plan sponsors of small group health plans that provide coverage via a contract with an issuer will opt to receive protected health information. The agency further assumes that it will take one hour to determine the procedural and organizational issues and 1/3-hour of attorney time to make plan document changes. The cost here would be $7.1 million.[13] It is hard to imagine a lawyer's bill for 1/3 of an hour.
- The agency assumes that it will take three hours for non-hospital providers to review existing business associate agreements and one hour in subsequent years. Hospitals will require 200 hours in the first year and 16 hours in subsequent years. Health plans will take 112 hours in the first year and 8 hours in subsequent years.[14]
- In the case where the requested information is pursuant to an administrative proceeding authorized by law, it is not clear from the regulation whether the burden lies with law enforcement to request the right information in its administrative subpoenas, or with the provider who has a new duty to make certain that 1) the information sought is relevant and material to a legitimate law enforcement inquiry, 2) the request is specific and limited in scope, and 3) de-identified information could not be used.[15] Putting aside the fact that a doctor must put on his/her law enforcement hat to figure out what a legitimate law enforcement inquiry is, there is no estimate of the costs for this activity.
- The costs presented for state and local government does not include an estimate or description of the impact on small local governments (e.g., local health clinics, local nursing facilities, county hospitals) as defined in section 601(5) of the RFA.[16]

5. The benefits analysis is a qualitative study that looks at several specific diseases like cancer and AIDS and then presents a theory that more individuals with those diseases will seek medical services if they have confidence that their records will be kept private. The presumption is that if more individuals seek early treatment, the diseases can be treated early, thereby reducing the cost of health care. Attempting to capture the inherent value of privacy by assuming that more individuals will suddenly seek medical care as a result of government regulations is not realistic. Perhaps the value could be better calculated by determining the actual cost of lost privacy. That is, how many have lost their jobs as a result of a privacy violation? How many have lost health insurance? How many were removed from school?

The privacy regulation is not the only regulation on which providers will have to focus. Aside from the myriad of existing regulations, providers are also facing eminent implementation of the electronic transaction standards regulation[17] that requires the health care industry to use standardized national drug codes when transmitting health care

[13] *Id.* at 82772.
[14] *Id.* at 82773.
[15] *Id.* at 82774.
[16] *Id.* at 82775.
[17] 65 Fed. Reg. 50311 (August 17, 2000).

data electronically.[18] The cumulative impact of regulations is a real threat to business survival and the overall economy. Regulators cannot regulate in a vacuum—every agency needs to be aware of the cumulative regulatory burden faced by the industries they regulate.[19]

Advocacy generally supports regulations that provide flexibility in implementation. However, HHS has spun a few lines of legislative text into a 370-page unwieldy mammoth in the *Federal Register*. In order to comply fully, providers will need greater assistance from the agency in untangling the web of requirements. In addition, a longer compliance period for at least very small entities would be beneficial. Advocacy understands that HIPAA only allows 3 years for health plans to comply and 2 years for everyone else covered by the regulation. Does HHS have general authority to extend this deadline? Can the date of "adoption" be modified or delayed?

Finally, Advocacy would like to bring to your attention what might be a minor technical error in the regulation. On pages 82,759 and 82,785 of the *Federal Register* (65 Fed Reg. December 28, 2000) there are references to providers that only maintain paper records and the fact that the regulation would not apply to them. This is not consistent with the agency's new policy of applying the rule's requirements to all records—electronic or written.

Thank you for your attention to these comments. Please do not hesitate to call our office if you have questions or if we can assist you in any manner, 202-205-6533.

Sincerely,

Susan M. Walthall
Acting Chief Counsel for Advocacy

Shawne Carter McGibbon
Asst. Chief Counsel for Advocacy

[18] Providers were successful in demonstrating that the transactions rule was too burdensome, but the agency did not take heed until the rule became final. Now, HHS is looking for a legal way to modify the rule's requirements. The lesson here is that careful consideration of burden needs to occur **before** rules become final. The privacy regulation deserves such careful consideration.

[19] HHS dismissed a commenter's complaint that the privacy regulation would be too much of a burden for those already struggling under the requirements of the Balanced Budget Act of 1997 (BBA) by stating that they "could not address the impact of the BBA or other statutes in the context of this regulation." 65 Fed. Reg. at 82592.