March 29, 2001

Comments of Peter Swire on the Medical Records Privacy Rule

Executive Summary

Thank you for the opportunity to comment on what course the Department of Health and Human Services should follow concerning the final rule on medical privacy that was published in the Federal Register on December 28, 2000 (the "December rule"). Under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), HHS was required to issue a final medical privacy rule by February 18, 2000. Despite this clear statutory requirement, some commenters have asked the Secretary to cancel the final rule and begin a new process of rulemaking.

My name is Peter P. Swire. I am currently a Professor of Law at the Ohio State University College of Law, where I am teaching courses on privacy and the law of cyberspace. From March, 1999 until January, 2001 I served as the Chief Counselor for Privacy in the United States Office of Management and Budget. During this time, I headed the White House working group on the medical privacy rule. The comments here are entirely in my personal capacity, and I have received no compensation for drafting them. I can be contacted by phone at (301) 213-9587, by email at swire.1@osu.edu, and my web site, containing publications and other information, is at www.osu.edu/units/law/swire.htm.

My recommendation is that Secretary Thompson allow the final rule to go into effect on April 14. For reasons explained below, *any other course of action should be understood as a repeal of the medical privacy rule, leading at best to a lengthy, indefinite, and unlawful delay.* In deciding not to repeal the rule, Secretary Thompson can simultaneously announce a speedy process for considering and making any specific changes that he believes are lawful and appropriate. This course will permit the current Administration to make any changes it believes are necessary while also protecting the confidentiality of Americans' medical records.

The comments here focus on a legal and practical understanding of the procedural history of the medical privacy regulation, based on my extensive involvement in drafting the rule. Analysis of this history leads to four key conclusions:

(1) The requirements of the Administrative Procedure Act are very demanding in light of the 52,000 comments already submitted and the large number of comments that would be submitted in a new round of rulemaking. Even if the Bush Administration makes this rule a major priority, it would likely take a minimum of one to two years before a new final rule could be issued. Implementation would then, under the statute, take place two years after that. *The first federal medical privacy protections would thus not be in place until 2004 at the earliest, and likely years later.*

(2) The bipartisan consensus in Congress has been to link two events: the HIPAA transaction rule, which creates standard protocols for sharing electronic medical records, and the HIPAA privacy rule, which ensures that confidentiality protections are an integral part of the new world of electronic health records. The final HIPAA transaction rule was issued last summer. Repealing the December privacy rule would violate the bipartisan consensus. *This repeal would be contrary to the intent of Congress. Medical records would be required to be shared freely, in electronic form, without the privacy protections that were always intended to accompany the unprecedented sharing of sensitive medical information.* If the December rule is repealed, privacy at best would be added later, as an afterthought to sharing procedures that would already be in place.

(3) *Repealing the December rule, while going forward with the HIPAA transaction rule, would be arbitrary and capricious and would be contrary to law in two respects. First, it is contrary to the statute to implement mandatory data sharing without the accompanying privacy protections. Second, repealing the December rule would lead to an illegal and lengthy delay beyond the HIPAA deadline that requires the rule to be in place now.*

(4) *Finally, repealing the December rule would be contrary to the statements on the issue by President Bush and Secretary Thompson.* During the Presidential campaign, now-President Bush said that he would "guarantee the privacy of medical and sensitive financial records." Secretary Thompson has said that "our goal is to achieve privacy protection that works," and he intends to "put strong and effective health privacy protections into effect as quickly as possible." There is a clear choice facing President Bush and his Administration. Permitting the December rule to go into effect will in fact guarantee the privacy of medical records. Canceling the rule, and opening the process to years of renewed debate, will not.

For all of these reasons, repealing the December rule would be illegal, unwise, and contrary to the statements on the subject made by President Bush and Secretary Thompson. A far better course is to allow the December rule to be implemented. HHS can also, based on its review of the comments due by March 30, 2001, announce a speedy timetable for proposing specific priority changes to the rule. By focusing on three, five, ten or some other number of specific topics, HHS creates a practical job for itself that can be done in a timely way and meet its key policy goals.

For instance, HHS might announce its specific proposed changes by July 1. The comment period might close by August 30. HHS could announce in the fall of 2001 the changes it expects to make. This timetable would allow covered entities a substantial period to plan and come into compliance before implementation takes place in early 2003.

As a matter of administrative law and practice, there is an enormous difference between making these specific changes and re-opening the entire rule. When making specific changes, HHS takes on a manageable task of considering comments on a specific issue and then

explaining its decision based on the record. By contrast, re-opening the entire rule requires the new leaders at HHS to determine their policy for every issue in the rule. It also creates the burdensome homework assignment of explaining each of those decisions based on the immense administrative record. To give a flavor of the difference, imagine the difference between rewriting and re-typing five pages of a thousand-page manuscript versus having to rewrite and re-type the entire thing. As any student can quickly grasp, the latter will take much, much longer.

These comments do not seek to repeat all of the reasons why the rule is good policy. These reasons are notably explained in the introductory pages of the rule itself, as well as in the materials released by the White House and HHS at the time of the December announcement. (These materials are available in the Presidential Privacy Web Archives of the Technology Policy Group, at www.privacy2000.org.) Based on my experience in drafting the proposed and final rule, these comments instead emphasize the enormous and foreseeable procedural problems that will result if the December rule is withdrawn. The comments do propose changes to the marketing provision and the rules governing pick-up of prescriptions on behalf of another person. The comments also discuss other important issues where change is not similarly justified: medical research; business associates; access by the government to medical records; applying the rule to oral and written medical information; and having a privacy official for covered entities. Finally, to rebut a number of inaccurate criticisms of the rule, I have attached a document by the Health Privacy Project entitled "Myths and Realities About HIPAA."

Discussion

Part I of these comments provides a timeline of how we have reached this point in the process. Part II explains why it will take so long to create a new proposed and final rule if the December rule is withdrawn. Part III shows why pulling back the December rule would violate the bipartisan consensus in HIPAA that the computerization of medical records must be accompanied by privacy protections. Part IV demonstrates why withdrawing the December rule would be contrary to law and subject to serious court challenge. Part V discusses what HHS should do next. The general approach should be to allow the December rule to go into effect while announcing an expedited process for making specific changes that HHS believes are lawful and appropriate. Part V also addresses what to do on specific substantive issues, including: marketing; pick-ups of prescriptions at pharmacies; medical research; business associates; access by the government to medical records; applying the rule to oral and written medical information; and having a privacy official for covered entities.

I. Timeline.

1996: Congress passes the Health Insurance Portability and Accountability Act (HIPAA). The law includes "administrative simplification" provisions that will require all covered entities to implement standard electronic protocols for sharing medical records. The statute also requires Congress to enact additional medical privacy legislation by August, 1999 -- a bipartisan consensus agrees that the computerized transfer of electronic medical records should only take place with privacy protections in place.

1997: As required by HIPAA, and after an extensive policy process within the Administration, HHS Secretary Shalala submits a detailed report to Congress on what proposed medical privacy legislation should include. This report gives all affected parties clear notice of the Administration's position on essentially all of the issues contained in the eventual final rule. Covered entities and the general public thus had from the fall of 1997 until February of 2000 to study the proposal, develop their position on each issue, and explain their views to the Congress, HHS, and the general public. Throughout this period, Congressional committees held a number of hearings on medical privacy, gaining comment on the major issues covered by Secretary Shalala's recommendations.

August, 1999: Congress is unable to meet the HIPAA statutory deadline for writing a medical privacy law. Despite significant efforts, especially in the Senate Health, Education, Labor, and Pension Committee, no medical privacy bill is passed by a committee or subcommittee. HHS thus gains, for the first time, authority to issue privacy rules under HIPAA. HIPAA states that final rules should be issued within six months, by February 18, 2000.

October, 1999: President Clinton and Secretary Shalala announce the proposed medical privacy rule and open it for public comment until December 30. At the strong request of both privacy and industry groups, as well as a number of members of Congress, the comment period is

then extended until February 15 so that careful and detailed comments can be drafted on the rule. In my view, this sort of modest extension of time, based on the request of a wide range of affected actors, is permitted under the statute. By contrast, repealing the December rule and beginning an entirely new proposed rule would violate the HIPAA requirement of promulgating a final rule by February, 2000.

February 15, 2000: Comment period closes on the proposed rule, with over 52,000 public comments. Administration forms a team of 70 people from over a dozen agencies to read and analyze the rules, and to create the detailed administrative record required to show the basis for each decision. Under the Administrative Procedure Act, a rule will be sustained in court only if the comments have received a thorough analysis and each policy decision is explained in the record. There is intensive and continuous work on the rule until the final rule is issued in December.

Summer, 2000: "Administrative simplification" or "transaction" rule announced. This rule creates standard protocols that must be used by covered entities to transfer medical records electronically. The Administration reiterates the bipartisan decision made in HIPAA, that administrative simplification must be accompanied by strong privacy protections. The transaction rule has estimated net monetary benefits of $2.9 billion per year for ten years, compared with the net monetary cost of $1.9 billion per year for the privacy rule issued in December. (Other benefits of the privacy rule, including the general preference of patients to have their records treated in a confidential manner, are significant benefits of the rule but are not estimated in monetary terms.) The HIPAA shift to mandatory electronic records, accompanied by privacy protections, thus has net monetary benefits of approximately $10 billion over ten years.

December 20, 2000. President Clinton and Secretary Shalala announce the final privacy rule, which is printed in the Federal Register on December 28. In the Federal Register the rule itself covers 30 pages, while the cost/benefit analysis and other accompanying material (including the responses to the over 52,000 public comments) covers 336 pages. The Federal Register states that the rule will become effective in 60 days. Under the terms of HIPAA, actual implementation would not be required until 24 months later, or February, 2003. That 60 day period for effective date is common for major rules, and also matches the 60-day period under the Congressional Review Act in which Congress can choose to override a major rule.

February, 2001. HHS discovers that the notice to Congress to trigger the Congressional Review Act was not sent in December as it should have been. My view, based on press reports and the information I have available, is that this was a simple clerical error, analogous to forgetting to attach the service of process to a brief. HHS sends the notice to Congress in February, 2001 and Congress has until April 14, 2001 to override the rule should it so choose. HHS also announces that it will receive public comments on the privacy rule until March 30, 2001.

II. Why It Will Take So Long to Create a New Proposed and Final Rule.

With this history in mind, it is clear that a number of factors make it an unusually lengthy process to draft a proposed and final rule in the area of medical privacy. Under the Clinton Administration, where the rule was a major priority, it took at least a year to create Secretary Shalala's recommendations in 1997, substantial work during the next two years to issue the proposed rule in October, 1999, and an additional fourteen months to complete the final rule in December, 2000. Congress, too, has found it difficult to act rapidly in this area, and indeed was not able to complete legislation within the three years provided by HIPAA.

Here are some reasons to expect that beginning a new rulemaking would prove a very lengthy process:

(i) *Many issues.* There are many distinct issues in the December rule. From my own experience, I estimate that there are at least dozens of policy and legal choices that would need to be decided by the new Administration if it decides to begin the rulemaking from scratch. In the Clinton Administration, there were many separate work-groups, usually with representatives of different Federal agencies, that met over a period of years to develop policy in issue areas such as medical research, patient access to records, workplace issues, and so forth. Creating a new process to address each of these issue areas, and each issue within each area, would be an extremely time-consuming task.

(ii) *Many comments.* The proposed rule received 52,000 public comments, many of which commented on numerous specific issues. The Clinton Administration assembled a team of 70 people from over a dozen agencies to read and respond to those comments. If there is a new proposed rule, then we would expect another large submission of comments, especially in light of the major media attention devoted recently to medical privacy. A new final rule would require careful analysis of: the initial 52,000 comments; the comments that are submitted this March; and the predictable tens of thousands of comments that will arrive in response to a second proposed rule. We know from the experience last year that it is a large and lengthy task to read, analyze, and respond to this magnitude of public comments.

(iii) *APA requirements.* Under the Administrative Procedure Act, HHS must have a rational basis in the administrative record for each of its policy decisions. It must also explain in the final rule how that rule responds to the public comments. The combination of many issues and many comments means that there are formidable APA requirements before a new proposed and final rule can issue. Failure to comply with these requirements would invite an overruling of the privacy rule in federal court, further delaying implementation of privacy protections. By contrast, the December rule carefully links each policy decision to the record and so should be resistant to this sort of APA attack.

(iv) *Complexity of issues and need for senior policy leadership.* Based on my experience, many of the issues in the December regulation are complex and require judgements

about technological, medical, legal, privacy, and other issues. Many of the issues also implicate multiple federal agencies. To resolve these sorts of issues often demands substantial involvement by senior policy officials in HHS and, for multi-agency issues, the Executive Office of the President.

Because the Administration has recently entered office, many of the relevant policy officials have not yet been named or confirmed. Once these officials are in place, there is an understandable period of time before they are fully up to speed, especially on the sort of complex issues involved in the privacy rule. In addition, a senior Office of Management and Budget official recently stated that the Administration does not expect to fill the position I occupied, as Chief Counselor for Privacy, in the Executive Office of the President. This lack of senior policy officials generally, combined with the decision not to name a responsible official for privacy, will pose a significant challenge to speedy completion of a new proposed and final rule.

Summary on length of time to draft a new rule. The comments here have shown reasons to believe that it will be extraordinarily difficult to draft an entirely new proposed privacy rule, receive comments on the proposal, and issue a final rule. Drafting a new rule, as requested especially by some industry groups, would require the Bush Administration to resolve many issues, respond to many comments, overcome major obstacles under the Administrative Procedure Act, and get priority attention from senior Administration officials, many of whom are not yet even in place.

Under the Clinton Administration, completing the medical privacy rule was a priority of the President, HHS Secretary Shalala, Chief of Staff John Podesta, and numerous other officials in HHS, the Executive Office of the President, and other federal agencies. Policy officials worked on medical privacy issues in the debate on HIPAA in 1996, in the course of Secretary Shalala's recommendations in 1997, and in the ongoing Congressional debates on the issue. With all of this preparation, and with devotion of a large staff to the proposed and final rule, it took from August, 1999 until December, 2000 (16 months) to complete the final rule.[1]

It is difficult to see why we should expect any shorter period for the new Administration if it decides to draft a new rule from scratch. If the new Administration were able to match the 16 month period to draft a rule – an optimistic scenario – then there would be no federal medical privacy protections in place until October, 2004.[2] Given the recent opposition to medical privacy protections from some quarters, together with the formidable homework required by the APA, it is quite possible that the Bush Administration would not complete the rule at all. *This analysis underscores the key conclusion made in the introduction to this comment, that a new rulemaking should be understood as a repeal of the medical privacy rule, leading at best to a lengthy and indefinite delay before any new rule can take effect.*

III. Pulling Back the Privacy Rule Would Violate the Consensus in HIPAA that the Computerization of Medical Records Must be Accompanied by Privacy Protections.

On the level of law, politics, policy, and common sense there is a compelling case for linking the computerization of medical records with the implementation of privacy protections. If the December rule is withdrawn, then this good policy will not happen. We will lose our best chance to build a computerized medical records system that makes sense.

An important part of HIPAA in 1996 was the creation of "administrative simplification." The experience of industry before 1996 was that the electronic transfer of records among providers, plans, and clearinghouses was not progressing well. There were no standard identifiers for health providers and plans. Even more importantly, industry was finding it very difficult to agree on standard protocols for exchanging medical data. The lack of standard protocols meant that computerizing health records was too expensive, and a company was reluctant to computerize on one standard if some of its business partners might choose to use a different standard in the near future, requiring costly retrofitting. For these and similar reasons, medical records were staying predominantly in paper form even as the rest of the economy was taking advantage of new computer technology to create efficiencies and better customer service.

In response to this problem, HIPAA required HHS to draft what is called the "transaction rule," which was issued in final form in the summer of 2000. This rule notably requires covered entities to use standard protocols for exchanging electronic medical records. The benefits of this rule are considerable. HHS estimated in its cost/benefit analysis that the net benefits would total $29 billion over ten years. The expected outcome of the transaction rule, together with other administrative simplification initiatives, will be to speed the computerization of medical records. Within the coming few years, we are likely to see the rate of computerization approach the norm in the rest of American industry. This is an historic shift from mostly paper to mostly electronic medical records. Our standard snapshot of medical records today is a file drawer behind a nurse's station. In the near future, it will seem odd unless the records are in a computer.

As the administrative simplification parts of HIPAA were being drafted in Congress in 1996, there was an extensive debate about how to protect patient privacy at the same time. There was a bipartisan consensus that it made sense to make privacy protections an integral part of computerizing the health care system. Congress considered placing detailed medical privacy provisions into HIPAA. Eventually, Congress decided instead to handle privacy in the following way. HIPAA required Congress to pass medical privacy legislation by August, 1999. If that deadline was not met, then HHS was required to issue a final privacy rule by February, 2000. With these deadlines, and in the rest of the legislative history, Congress went out of its way to indicate the importance of having privacy protections implemented in tandem with the administrative simplification measures.

Linking computerization and privacy protections is not simply the intent of Congress. There are strong policy reasons to link the two. The computerization of medical records, while bringing many benefits, also creates new and substantial privacy risks. For instance: (i) Copies

of records can be made with a click of a mouse rather than through laborious, page-at-a-time copying of paper records. The cost and ease of copying decline greatly, and it is much easier to transfer electronic files to remote locations. (ii) Computer systems are typically much more subject to attack from outsiders than are physical records. The recent incidents at the University of Washington Medical Center and elsewhere show that it has been quite easy for skilled hackers to gain unauthorized access to large numbers of medical records. (iii) Medical records in computer systems, unless accompanied by unusually good security, are also vulnerable to improper access by employees or others who have access to the computer systems. These "inside hackers" can often gain access to far more computer records, with lower chance of detection, than with paper records. (iv) The lower cost of copying and transferring computer records speeds the trend in modern medicine to more different organizations having access to a patient's medical records (providers, insurers, auditors, researchers, etc.). Where cost has been a barrier to sharing of information in paper-based systems, the lower cost of computer records will mean that information is shared more often.

The common sense of patients reinforces these policy points. Already, in our primarily paper-based medical system, polls show that one in six patients have refused to report honestly to a medical provider due to fears about confidentiality of records. This number is likely to rise sharply in the future if patients see that medical records have been computerized without having privacy protections in place. The reluctance to report accurately to a provider can lead to terrible medical outcomes, from a refusal to get an HIV test to fear by a mentally ill patient to speak truthfully to a psychiatrist. In the detailed cost-benefit analysis of the December rule, HHS documented billions of dollars of medical benefits that would result from patient willingness to report truthfully to a provider.

From a technological point of view, it also makes far more sense to build a computer system properly from the start than to patch changes onto the system later. If we implement administrative simplification now and privacy later, then privacy will be a retrofit. It will cost more money and be done less well than if privacy had been built into the system from the start. At the risk of sounding too cynical, it is easy to imagine the following argument being made by some industry actors in the future: "Now that we have built our new computer systems, and complied with the administrative simplification requirements, it is too expensive and not even feasible to go back and re-program those systems for these new privacy regulations." The form of this argument is known as the "double bind": it is too early to issue the privacy regulation now because it requires further study, and it will be too late to issue the privacy regulation later because the computer systems will be locked into place.

A related point is that industry should expect to adopt good practices as part of the overall computerization of health records. If firewalls are part of the privacy and security rules, then implementing firewalls should not be seen as the "fault" of the regulations. Firewalls are good practice in industry generally, and it would be irresponsible to establish a large system filled with sensitive records and not have basic safeguards in place. Many aspects of the privacy rule are simply common sense for handling sensitive information in a computerized environment.

Summary on the link between computerization and privacy. The discussion here shows that the link between computerizing medical records and ensuring privacy is based on the bipartisan agreement in the HIPAA statute, the new risks to privacy that come from computerization, and the common sense of patients who will recognize the risks of switching to computerized records unless privacy safeguards are included. As a matter of computer system design, it also makes far more sense to build privacy in from the start rather than trying to patch privacy rules later onto an already-existing system.

IV. Why Withdrawing the December Rule Would Be Contrary to Law.

It would be unlawful for HHS to withdraw the December rule and begin a new medical privacy regulation for at least two, and possibly three, reasons. First, HIPAA requires that the transaction rule and the privacy rule be implemented at the same time. Second, withdrawing the December, 2000 rule would violate HIPAA's statutory deadline for prompt promulgation of a privacy rule. Third, it is possible that under the Administrative Procedure Act the December rule should be understood as already being in effect, so that withdrawal of the December rule would be unlawful unless additional steps are taken under the Administrative Procedure Act.

First, for reasons discussed in Section III, the clear intent of HIPAA was to have the privacy rules implemented at the same time as the administrative simplification rules. Permitting the administrative simplification rules to go forward, while the privacy rules are indefinitely delayed, would be contrary to the statutory language and intent. Implementing the transaction rule without privacy would also be arbitrary and capricious. To mandate the computerization of records under the transaction rule, while omitting the necessary privacy protections, would lead to an unreasonable outcome that would have predictable and apparent negative effects.

Second, withdrawing the December, 2000 rule would be contrary to HIPAA's requirement that the final medical privacy rule be promulgated by February, 2000. It may sound odd to state that the December, 2000 rule is lawful despite missing the deadline by eight months, but any new delay would be unlawful. I believe, however, that this is precisely the case.

The December, 2000 rule is lawful under the deadline because of the reasons why HHS did not meet the February, 2000 deadline. As stated above, HHS first gained the power and duty to issue the regulation in August, 1999. HHS issued the proposed rule in October, 1999, which was a prompt response to its receipt of regulatory authority. HHS originally asked for comments by December, 1999. HHS then received letters from a wide range of actors, including both privacy and industry groups, that uniformly asked for more time to prepare comments on the proposed rule. In response to this request, HHS extended the deadline for comments for 45 days, into February, 2001.

As stated above, HHS received over 52,000 public comments on the proposed rule. This total is likely far greater than most Members of Congress would have expected when the

original deadline was set. In any event, the Administration promptly formed a large team of 70 persons to read, analyze, and respond to this large set of comments. In light of the statutory deadline and the Administrative Procedure Act, which requires reasoned responses to public comments, HHS acted reasonably as it conscientiously prepared the final rule, which was issued in December, 2000. In light of the prompt and continuous action by HHS after receiving regulatory authority in August, 1999, I believe the timing of the issuance of the final rule in December was in compliance with the statute.

The analysis changes entirely, however, if the December rule is withdrawn. For reasons given in Part II above, withdrawal of the December rule should be understood to be repeal of the medical privacy rule. At a minimum, there will be a long and indefinite delay before HHS can issue a new proposed rule, receive thousands of new comments, and then issue a new final rule that responds to all of the comments.

This sort of long and indefinite delay, after a final rule has already been issued, is contrary to the deadline in HIPAA. In other cases, courts have imposed various equitable remedies against federal agencies that have failed to comply with statutory deadlines when promulgating regulations. In this instance, there are at least two remedies that a court might consider. First, the court could find that the December rule continues in effect until and unless HHS promulgates a different final rule that complies with HIPAA. In this event HHS would retain the ability to change the medical privacy regulation, but there could not be the indefinite delay that would otherwise result from withdrawing the December rule. As a second remedy, the court might decide that implementation of the transaction rule should be stayed pending promulgation of a final privacy rule. This remedy would avoid the unlawful result of requiring the computerization of medical records without the accompanying privacy protections. This remedy would also give the various parties an incentive not to have further delay in promulgating the privacy rule – industry that favors the transaction rule in order to speed computerization would understand that privacy protections are a required part of that computerization.

Third, further research is needed to determine whether the December rule actually took effect in February, 60 days after publication in the Federal Register. The Congressional Review Act requires Congress to have 60 days after being notified in order for Congress to decide whether to override a major rule. The open question is whether the Congressional Review Act also disrupts the effective date for purposes of the Federal Register and the Administrative Procedure Act. In this case, the Federal Register notice in December contemplated having the rule take effect in February. If a court finds that the rule did take effect in February, then additional steps are required under the *State Farm* case before that rule can be repealed.

V. What HHS Should Do Next.

(A) The general approach. Instead of unlawfully withdrawing the December rule, there is an alternative approach that complies with the statute while meeting other important goals. This approach would permit the December rule to enter clearly into effect on April 14,

2001. No action would be required of HHS. Administrative action is only required if Secretary Thompson wishes to repeal the December rule.

Either before or after April 14, Secretary Thompson could also announce a plan for making specific changes to the December rule. These changes would be amendments to the final December rule. HHS can announce a speedy timetable for proposing specific priority changes to the December rule. By focusing on a limited number of priority topics, HHS creates a practical job for itself that can be done in a timely way and meet its key policy goals.

For instance, HHS might pledge in April to announce its specific proposed changes by July 1. The comment period could close by August 30. Because the comments would only address a limited number of issues, it would be manageable to review the comments and issue a final rule within a matter of months. This timetable would allow covered entities a substantial period to plan and come into compliance before implementation takes place in early 2003.

A provision of HIPAA limits changes to its regulations to once per year. The possibility therefore arises that the revisions would be completed before a year had passed since the previous rule. In this event, there is nothing to prevent HHS from announcing publicly in advance what it plans to make official when it is allowed to do so. This sort of public announcement would give covered entities the maximum time to plan their compliance.

As a matter of administrative law and practice, there is an enormous difference between making these specific changes and re-opening the entire rule. When proposing specific changes, HHS takes on the achievable task of considering comments on a specific issue and then explaining its decision on the record. By contrast, re-opening the entire rule requires the new leaders at HHS to determine their policy for every issue in the rule, and to ensure that all of the inter-locking pieces of the rule fit properly together. It also creates the burdensome homework assignment of explaining each of those decisions based on the immense administrative record. To give a flavor of the difference, imagine the difference between rewriting and re-typing five pages of a thousand-page manuscript versus having to rewrite and re-type the entire thing from scratch. As any student can quickly grasp, the latter will take much, much longer and involve far more work.

This approach of targeted changes has other advantages. Permitting the December rule to go into effect is the best and only way to give effect to President Bush's promise to guarantee the privacy of medical records. This course reaffirms the importance of privacy protection and avoids the violations of law discussed in Section IV above. It lets covered entities know that they should be planning to implement privacy protections in the foreseeable future rather than signaling that there may be indefinite delay. At the same time, the targeted changes provide the Bush Administration an opportunity to exercise its discretion as to important policy issues. As discussed below, I suggest some changes to the December rule in light of the comments since its release. It is not surprising that there can be improvements to a project of this magnitude. Continued improvement, however, is more likely to come from experience in implementing the

rule rather than in a long and indefinite delay. In the course of implementation, covered entities will uncover what works well and what not so well in the regulation.

(B) Specific substantive issues.

I now turn to specific substantive issues under the rule. For a project of this magnitude, there are inevitably ways to refine and improve a rule over time and it makes eminent sense for HHS to seek such improvements. However, based on my experience in the rulemaking process and my review of the criticisms to date, I have been disappointed by the inaccurate nature of many of the criticisms of the December rule. For that reason, I have attached a document written by the Health Privacy Project entitled "Myths and Realities About HIPAA." That document rebuts a number of inaccurate criticisms of the rule. In general, great caution is due before accepting broad claims that the final rule is unworkable. As the timeline in Part I indicates, there has already been a multi-year process in which all affected groups submitted detailed comments. Numerous refinements have already been made to each part of the rule in response to these comments. Rewriting the rule from scratch runs the risk that new problems will creep in that have already been addressed in the December rule.

Below, I suggest changes that should be made for the "marketing" provisions and with respect to picking up prescriptions for another person. I then examine a number areas where major changes are not required, including ; medical research; business associates; access by the government to medical records; applying the rule to oral and written medical information; and having a privacy official for covered entities.

(i) "*Marketing.*" A number of criticisms have been made of the provisions concerning "marketing" in Sec. 164.501 and Sec. 164.514(e). As an initial matter, I wish that the rule referred to these activities as "communications with a covered entity's own patients" or "communications with patients." That is my understanding of the intent of the marketing provisions and of the text of the regulation. Changing the name of this part of the rule would reduce the confusion.

My understanding of the December rule and the intent of the December rule is that the "marketing" provisions explain how a covered entity, such as a doctor or hospital, can communicate with its own patient with respect to goods or services offered by the covered entity or a third party. My understanding here is that information about patients can be transferred to third parties only when the third party is acting as an agent for the covered entity. For instance, a doctor might hire a service to handle her mailings to her own patients. If the doctor decided to do a "marketing" mailing to her patients concerning a medical newsletter, the outside service could perform the mailing to patients. (The outside service would therefore receive the names of patients who get the mailing). The outside service, however, would be under a business associate contract not to use those names for other purposes. In this example, the outside service is acting much like a doctor's secretary – someone other than the doctor sends out the actual mailings, but

the mailings are being done to the doctor's patients at the doctor's direction. The December rule also includes a number of safeguards for such mailings. For instance, the mailing must clearly identify that the mailing is coming from the doctor, and the mailing must indicate if the doctor is being remunerated for making the mailing.

There are badly drafted sentences in the December rule that can lead a reader to believe that the rule permits a third party to receive a patient's medical records in a broader range of circumstances. Some have suggested that the third party can then market to the patient on its own behalf. I do not believe that is a correct reading of the December rule. But redrafting of the relevant sections can make the intent more clear, and this should be done.

Another issue under the marketing section is whether the opt-out should be available to patients only after the initial mailing is made. Some analogous sections of the rule, such as for directory information and visits by clergy, indicate that an opt out should occur at an earlier time, before the unasked-for contact takes place. HHS might consider whether to have the opt-out apply before the communication to the patient takes place.

(ii) *Pharmacy pick-ups.* One of the most common criticisms of the December rule is that it would make it difficult for family members or friends to pick up pharmacy prescriptions on behalf of another person. This provision should be fixed.

Section 164.506 sets forth the general rules concerning consent for uses or disclosures to carry out treatment, payment, or health care operations. The general rule is that a provider must obtain the individual's consent prior to using or disclosing protected health information. The question is how to get that prior consent from the patient if a different person has stopped at the pharmacy to pick up the prescription. One route under the December rule would be to find that there are "substantial barriers to communicating" with the patient, and that in the "professional judgment" of the pharmacist the patient's consent to receive treatment "is clearly inferred from the circumstances." Sec. 164.506(a)(3)(C). Although this language may support the pharmacy's decision to provide the prescription, a revised provision could make that authority more explicit.

A broader question is what should be inferred from the bad drafting of the rule with respect to picking up prescriptions. *Critics of the rule try to use this example to indicate that the entire December rule is riddled with unworkable provisions. I think the repeated mention of the prescription pick-up issue shows just the opposite. Critics mention the prescription problem so often precisely because of the small number of similarly valid criticisms.* Once again, I urge the reader to review "Myths and Realities About HIPAA," which in a common-sense way rebuts other charges that have been leveled against the December rule.

(iii) *Medical research.* There is broad bipartisan support today for progress in medical research, not unlike the broad support for protecting the confidentiality of individuals' medical records. The question is how best to achieve both of these goals. In the final rule, there are three

choices for conducting medical research consistent with privacy. First, patients can consent to release of their own records for research. Second, any sharing of medical records is permitted when the records have been "deidentified" under the rule. Third, any research is permitted where the research project has been approved as ethical by an Institutional Review Board or similar private-sector entity. In light of these three paths for permitting medical research, a heavy burden should be on critics of the rule to explain in detail how, if at all, the final rule prevents legitimate medical research.

(iv) *Business associates.* It is easy enough to understand why business associates must be included within the privacy protections of the rule. If only covered entities themselves were affected, then the exceptions would truly swallow the rule. A hospital, for instance, would be able to hire a computer firm to handle all its medical records. That firm, in turn, could post *all* patients' records directly to the Internet, because the firm would not be a covered entity as defined by HIPAA. In order to avoid this absurd result, which Congress did not intend to create, HHS correctly provided that covered entities as well as their business associates should be under an obligation to protect patients' medical records.

Legitimate questions have arisen about how to govern the relationship between covered entities and business associates. Under the proposed rule, for instance, covered entities would have had an obligation to "monitor" the privacy activities of their business associates. Industry comments explained legal and practical concerns about this approach. In response to these industry comments (and as one example among many of ways in which the proposed rule was refined during the comment process), the final rule states that the covered entity is responsible for violations only where it actually knows of a pattern or practice of material violations by the business associate. Sec. 164.504(e)(ii). It is reasonable to expect action by a covered entity when it has actual knowledge of important violations of privacy promises by its business associate.

Questions have continued about why covered entities are expected to have contracts with their business associates. The answer is simple -- if the confidentiality of patient medical records is ever to be protected, then there must at some point be an understanding of what recipients of medical records can and cannot do with those records. The burden of creating these contracts can be easily overstated. It is good industry practice already in many instances for a contract to specify how patient records are to be handled, and standard contracts will continue to develop for many industry sectors. Such contractual understandings are completely routine in modern business practice for the handling of other information, such as trade secrets, copyright, and other intellectual property. Furthermore, given the two-year minimum before HIPAA rules are implemented, the drafting of privacy provisions can be done in many or most cases as part of the regular cycle of forming and renewing contracts with business associates.

In short, business associate provisions are essential for the rule to make sense, have been made more workable in response to industry comments, and can be implemented far more easily than some have charged. That said, there may be simpler ways to put business partners on

notice of their responsibilities to handle records well without the need for an extensive contract with each covered entity. For instance, business associate responsibilities in a given case might be incorporated by reference. The parties would simply indicate that they are business associates under HIPAA. This approach would reduce contracting costs while keeping the essential point that a business associate cannot be a route to leaving sensitive medical records unprotected

(v) *Access by the government to medical records.* There have been perhaps inadvertently inaccurate statements that the December rule would harm privacy due to new access by the Federal government itself. For instance, Representative Armey has written a letter stating that the rule "would put the health privacy of millions of Americans at risk." The letter criticizes "the rule's new mandates requiring doctors, hospitals, and other health care providers to share patients' personal medical records with the federal government, sometimes without notice or advance warning." As alleged support for its claims, the letter cites to Sec. 160.310, which does indeed provide the *only* requirement in the regulation for new disclosure of medical records to the government. The disclosures under that section are for compliance reports "as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity has complied or is complying with the applicable requirements" of the rule. That is, disclosure is only what is "necessary" to determine compliance. My own reading of that language would suggest that compliance reports could generally be made without revealing any patient's personal information. Moreover, I think there is little doubt that covered entities and privacy advocates will object strongly and successfully if these compliance reports compromise patient privacy.

Rep. Armey's letter also expresses concern about records being released "sometimes without notice or advance warning." The rule specifically states that such access is authorized "if the Secretary determines that exigent circumstances exist, such as when documents may be hidden and destroyed." Such a finding would need to be made in advance, on a case-by-case basis, and subject to judicial review after the fact in case of dispute.

The only required new government access to records under the rule is thus in the limited number of actual enforcement actions for privacy violations. On the other hand, the rule creates numerous new privacy protections for medical records that apply equivalently to government and private-sector entities. The rule also creates specific new privacy protections for law enforcement and other uses of records that apply only to the government. The December rule protects privacy, and it does not put Americans' privacy "at risk" due to new access by the Federal government.

(vi) *Applying the rule to oral and written medical information.* The proposed rule would have applied to records in electronic form as well as the information in those records even if kept in written form or known to the provider. The proposed rule also specifically solicited public comment on the issue of whether to apply to oral and written protected health information generally. In response to the comments, HHS decided that it was lawful and appropriate to apply the December regulation to protected health information regardless of whether the information is

placed in electronic form.

The logic of this decision is clear enough. Privacy protections should apply to oral statements. It would be bizarre to have a privacy rule that would allow a psychiatrist to divulge all of a patient's statements so long as they were oral statements and not written down. Similarly, privacy protections should apply to written records. It would be bizarre if the results of HIV tests were unprotected whenever they were recorded on paper. In addition, as pointed out by public comments on the proposed rule, there would be substantial burden issues if covered entities kept two sets of records, one set for electronic records covered by HIPAA and a separate set for other records.

Although the rule clearly should cover health information in oral and written form, it is possible that there are specific situations where some amendment to the rule would be appropriate to respond to different circumstances that arise for oral and written records. Certain practices may differ for oral, written, and electronic records. I suggest that the Secretary seek comment on whether any such differences would justify different treatment in some circumstances for electronic records and other protected health information.

(vii) *Privacy official.* In the Regulatory Impact Analysis for the December rule, a major cost item is the requirement that each covered entity name a privacy official. The rule makes clear that there is no expectation that this be a full-time job, especially for smaller organizations. But the cost of having a person responsible for privacy issues is significant when a modest number of hours per year for this job is multiplied by the number of covered entities. In order to reduce the amount of "cost" for the privacy rule, it may therefore be tempting for the new Administration to no longer expect covered entities to have a privacy official.

I recommend against this change. One reason is that there needs to be a responsible person for patients to contact when they seek access to their medical records. Even some industry groups that have opposed other parts of the rule have agreed that there should be some regime for patients to have access to their medical records. If this regime exists, then there should be a point of contact in the covered entity for making access requests.

More generally, I believe that appointing a privacy official should not be properly understood to be a cost of the rule. Instead, having such a person is an expectable part of the good practice of handling sensitive medical information in a computerized environment. As computer systems are designed and implemented for medical records, someone in the organization should be keeping track of how confidentiality and security are being handled. The baseline expectation should be to have a privacy official. Even if there is no regulation requiring the naming of a privacy official, I believe responsible medical entities will name one. In assessing the cost of requiring this, the cost for purposes of the Regulatory Impact Analysis should be the extra number of privacy officials if their existence is made a requirement. That number is likely to be modest. Furthermore, the greatest impact of the requirement will likely be to improve privacy in those organizations that would otherwise ignore the issue by not having a

person responsible for it.

ENDNOTES

1. HHS received authority and responsibility to issue a regulation in August, 1999, when Congress was not able to meet the HIPAA deadline for medical privacy legislation. In fact, a substantial amount of the work for the proposed rule was done before August, 1999 in light of the (correct) perception that Congress would have trouble meeting that deadline. The estimate of time needed to draft the proposed rule, therefore, is very conservative, and it actually took well over 16 months from the time of beginning to draft the proposed rule until issuance of the final rule.

2. This calculation assumes that HHS would begin the new process immediately, in April, 2001. Sixteen months later would be August, 2002. Sixty days to comply with the Congressional Review Act would be October, 2002. Twenty-four months before implementation is expected, as required by HIPAA, would be October, 2004.