HIPAA Administrative Simplification: Standards for Electronic Health Care Claims Attachment, Proposed Rule [45 CFR Part 162]

Comments of the World Privacy Forum, Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC), PrivacyActivism, Privacy Rights Clearinghouse, and U.S. Public Interest Research Group (U.S. PIRG)

Via http://www.cms.hhs.gov/regulations/ecomments and express mail.

Centers for Medicare and Medicaid Services
Department of Health and Human Services
Attention:CMS-0050-P,
Mail Stop C4-26-05,
Baltimore, MD 21244-1850

November 18, 2005

Re: HIPAA Administrative Simplification: Standards for Electronic Health Care Claims Attachment, Proposed Rule. [45 CFR Part 162] [CMS-0050-P]

Pursuant to the notice published in the Federal Register on September 23, 2005 regarding HIPAA Administrative Simplification: Standards for Electronic Health Care Claims Attachment, Proposed Rule [45 CFR Part 162] [CMS-0050-P], the World Privacy Forum and the Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC), PrivacyActivism, Privacy Rights Clearinghouse, and U.S. Public Interest Research Group (U.S. PIRG), ("The Submitters") respectfully submit the following comments.

The comments are divided into three sections. Section one, "General Comments," includes general comments about the Notice of Proposed Rule Making (NPRM). Section two "Specific Comments" includes comments relating to specific sections of the NPRM. Each comment in section two begins with a label per the NPRM instructions, such as DEFINITIONS, or COSTS and includes the outline number and page number as it appears in the NPRM. Section three is a brief conclusion.

I. General Comments on the Notice of Proposed Rulemaking

The Department of Health and Human Services (HHS) seeks to assist the transition of the healthcare sector from a paper-based process to an electronic data interchange (EDI) based process.[1] The submitters contend that not enough attention has been paid to protecting patient privacy, choice, and security in this process. Specific areas of concern in the Healthcare Claims Attachment NPRM include those relating to the impact on the Privacy Rule, the standards making process, balancing goals of EDI adoption with privacy, protecting the minimum necessary rule in spirit and in practice, issues related to solicited attachments, and cost and savings assumptions, among other issues.

A. General Comments on the Standards Process and Outcomes

We understand that the NPRM reflects years of work by the many individuals, corporations, and stakeholders involved in the standards processes discussed in the NPRM. However, the shortcomings in this standards process have excluded some stakeholders, in particular, stakeholders in the privacy community.

Few, if any, non-profit privacy organizations have the practical ability to actively participate in the standards process due to the costs associated with such participation. Membership in ASC X12N for nonprofit organizations is $2,500 a year. In addition to this recurring fee, there are additional costs of attending the X12 meetings, which are held around the country and add thousands more dollars in travel-related costs. Participating in HL7 would add another tier of membership and travel costs. While these costs may be manageable for some large non-profit organizations, privacy groups are typically small organizations with budgets that do not realistically allow for such expenditures.

To actively participate even as a non-member is also expensive. For example, to simply read the X12 and UN/EDIFACT publications costs thousands of dollars,

[1] In our use of the term Electronic Data Interchange or EDI in these comments, we using it in its broadest sense and are including XML in our definition.

according to ASC X12N. Some of these documents are free for members or are offered at a lower price for members. For non-members, the fees can be substantial.

Thus, the standards processes that HHS relies upon in setting basic rules that directly affect privacy and security of patient information are structured so that privacy perspectives are unrepresented. This exclusion of privacy perspectives may not be intentional, but the result is the same. Important perspectives are absent, and that absence damages the legitimacy of the standards process, leads to unbalanced results, and may ultimately impede public acceptance of HHS actions that rely on standards. As HHS moves toward the establishment of increased computerization and networking of health records, it cannot afford to allow relevant views to be routinely overlooked as standards are developed.

Privacy must be incorporated into the standards making process from the beginning of the process all the way through to the final outcomes. While the privacy community values the NPRM process and the rights the process affords, in the case of NPRMs that incorporate industry consensus standards, the standards process must be genuinely and practicably open from the beginning, or the stated goal of conducting an "open" standards process cannot be met. It is insufficient that privacy groups can only comment after the standards process is complete – privacy is not something that can simply be tacked on at the end of a long process.

The best way to accomplish an open standards process that includes privacy is to involve privacy organizations from the beginning of that standards making process, and to incorporate privacy viewpoints throughout the standards setting process. We request that HHS remedy the shortcomings in this process in such a way that will ensure the participation of interested privacy organizations.

To accomplish this, we specifically ask that HHS insist that standards groups incorporate more privacy awareness in the standards through the direct involvement of privacy groups in the standards process, and by reaching out actively to the privacy groups. We also ask HHS to mandate that standards groups affirmatively disclose all privacy, patient, and consumer groups that participated in the standard development. We

also ask HHS to require standards groups to document their affirmative steps to bring privacy, consumer, and patient groups within the process.

B. General Comments on Goals of Standardization

The goals HHS articulates in the NPRM of having a more automated, standardized approach to health care information exchange must be balanced by privacy, patient choice, and security concerns. Finding a way to protect privacy, patient choice, and security is particularly important as health information formats transitions to automatically adjudicated models. This includes healthcare claims attachments.

C. General Comments on Cost

The cost estimates set forth in the NPRM are not appropriately substantiated and are therefore not reliable. HHS' estimates of cost savings is based on a single 1993 WEDI report coupled with "conservative assumptions" from the Transaction rule to predict costs and savings. The NPRM states that some of the cost estimates were based on "informal discussions with industry representatives of health plans and vendors."

A grouping of 12-year old data, "conservative assumptions," and informal discussions with industry members is not an appropriate factual basis upon which to rest either a broad assertion of cost saving or specific costs and savings assumptions. Another concern is that HHS did not use an important August 2005 WEDI report on healthcare claims attachments in its estimates, a report that if used would have changed the cost estimates, particularly the savings.

D. General Comments on the Privacy Rule and the Minimum Necessary Standard

The current approach of the NPRM does not adequately protect the minimum necessary standard because health providers are not always able to redact electronic content at a sufficiently granular level due to limitations imposed by some vendors' systems. The minimum necessary standard, as articulated in the Privacy Modification Final Rule [§164.502 (b)(1)] requires a covered entity to make reasonable efforts not to

use, disclose, or request more than the minimum amount of Protected Health Information (PHI) than is necessary to accomplish the intended purposes of the use or disclosure. As HHS promulgates rules promoting broad adoption of electronic interchanges of data, the minimum necessary standard needs to be protected in all interchange scenarios, including digital formats. To accomplish this in practice in healthcare claims attachments, it will be necessary for health providers to be able to easily redact unnecessary information from electronic documents at a very specific level, for example, editing content line by line – something that is currently challenging for many providers.

It is, for example, a common practice of physicians when dealing with paper medical files and related records to remove the paper documents that are unnecessary for the adjudication of a health care claim. The patient correspondence section of a medical file will not always be necessary to send to a health plan. If such a correspondence is relevant, only the relevant pieces of correspondence would be sent.

However, in electronic format, the information selection and "publication," or "printing to an electronic file" process [2] has many imperfections due to restrictions imposed by some vendor software. In the EDI environment, providers do not always have the ability to create an electronic medical file with control over specific content at a sufficiently granular level, as opposed to control over which entire sections of a file should be included in the file.

For example, a provider may need to submit the central medical data set from a file to a health plan along with an attachment. As previously discussed, in a paper format, providers can manually remove the pieces of paper in the data set and attachments that are not necessary. However, when a provider has to "publish" and share the central medical data set and attachments electronically, the provider may not be able to edit the content level of the data to a deep enough level to permit the removal of unnecessary information embedded within the data set. For example, in some major vendor software, a physician can only include an entire data set or attachment with no content-level edits in the electronic version of the medical file. That is, the physician cannot remove unnecessary information at the paragraph level.

---

[2] The term "publishing" in these comments refers to a term or art that providers use when changing a medical file into one or more electronic formats for internal use or for use in billing and providing patient care.

As a result, information that a provider would not have sent in paper format often is sent in electronic format. This issue is frequently beyond the control of the provider. This problem is further exacerbated in the case of scanned documents that may contain abundant data not directly connected to a claim.

The end result of these challenges is that the "minimum necessary" standard is being diluted in the EDI environment. Providers do not intentionally set out to dilute or circumvent the minimum necessary rule, and many providers struggle with software systems and vendors in their efforts to comply with the rule. But vendors do not have motivation to change their systems.

We ask that HHS include in the healthcare claims attachments rulemaking a requirement that health providers have the capability of line-level editing and paragraph-level editing throughout the entire content of a published electronic medical file or health record or attachment. If HHS does not mandate this capability, then vendors will not have to make it available. We recognize there will be a cost associated with this requirement, but the cost will be amortized over millions of records and over a long period of time. This requirement does not need to go into effect immediately, but the requirement should be stated in the final rulemaking and industry should be allowed sufficient time to comply. At a minimum, HHS should mandate that new systems include granular editing capabilities. If it is not practical to mandate the same requirements for some or all legacy systems, HHS should nevertheless define the requirements for the future.

HHS has the opportunity with this rulemaking to give those making healthcare decisions the power and ability to carefully edit at a granular, paragraph by paragraph level, electronically published health records and attachments. Health care providers need and require more detailed control over the content aspect of electronic publication of medical files. This will enhance privacy for patients, and may help to increase patient trust in electronic systems.

II. Comments on Specific Elements of the NPRM

In our specific comments, we have retained the original NPRM outline numbers for clarity, and we have used the HHS section descriptions where available. The page numbers refer to the original NPRM page numbers.

Section II: Provisions of the Proposed Regulations p. 55993

A. DEFINITIONS p. 55993

(3.) Clinical reports definitions p. 55994

Scanned files that become claims attachments introduce special problems in regards to rigorously excluding psychotherapy notes from clinical reports in actual practice. The NPRM states that: "Clinical reports means reports, studies, or notes including tests …. Clinical reports do not include psychotherapy notes" (p. 55994). In the case of covered entities that choose to use scanned images (documents) as attachments, there is the possibility that a scanned document with necessary information such as lab reports or studies may also contain psychotherapy notes. It is unreasonable to expect that that this situation will never arise, particularly in the case of scanned files.

Compounding this fundamental challenge, a further difficulty arises after the attachments are sent to a health plan. A majority of respondents in the August 19, 2005 WEDI/HL7/X12/AFEHCT National Healthcare Claims Attachment Survey Final Report stated that scanned attachments, after being sent to a health plan, are "Almost Always" saved and stored (WEDI 2005 Survey, p. 44).

Scans stored in a database can lead to increased potential for misuse or patient harm beyond the initial claims attachment adjudication process. Unfortunately, there are already examples of health plan database breaches. Medica Health Plans (Minnesota) experienced a database breach in 2005 that affected 1.2 million individuals. In this situation, hackers stole sensitive and confidential data from Medica's computer system two times in January 2005 and shut down parts of the system on four other occasions, exposing members' SSNs, addresses, dates of birth, employment information, and names

of relatives.[3]

We urge HHS to acknowledge the challenges scanned files introduce and find a way of addressing this problem in the final rulemaking so that psychotherapy notes do not get inadvertently attached as an image file of a larger document and then subsequently stored at a health plan. HHS may need to mandate fine-grained editing capacities for software tools so that psychotherapy notes can be redacted. It may also be advisable to require periodic audits of stored records to purge psychotherapy notes.

C. OVERVIEW OF KEY INFORMATION FOR ELECTRONIC HEALTH CARE CLAIMS ATTACHMENTS p. 55994

It is not feasible to properly evaluate HHS' claims regarding the impact of increased computerization and networking without better information. The NPRM states that: "This proposal has the potential for helping the industry attain desired efficiencies, expedite payments, reduce fraud and abuse, and improve the accuracy of medical information" (p. 55995 paragraph 2).

If attaining efficiency, expediting payments, reducing fraud and abuse, and improving the accuracy of medical information are the stated goals of the NPRM, then a formal study and regular, public reporting of specific outcomes in all of these areas should be mandatory in order to provide a factually determined basis for these statements. We therefore request that HHS formally undertake a sector-wide study and subsequently publicly report on the efficiency, abuse and fraud reduction, and accuracy improvement claims made in this NPRM.

It is also essential that more information be available on the costs and benefits of health information systems. If HHS ultimately contemplates the expenditure of tens of billions of dollars on health care information technology, then HHS must prove to the public that these dollars will be well spent.

---

[3] See <http://www.securityinfowatch.com/online/Cabling--and--Connectivity/Medica-Health-Plan-Alleges-that-Former-Employees-Hacked-Sensitive-Data/4484SIW422>.

(5.) ELECTRONIC CLAIMS ATTACHMENT TYPES p. 55996

The process of deciding on the six types of claims attachments went through a multi-year process and through pilot programs with a great deal of industry input. While this is completely appropriate, any future electronic claim attachment types need to be decided upon after greater outreach to smaller stakeholders and a wider variety of stakeholders, including the privacy community. HHS should establish a specific and verifiable process to ensure that privacy stakeholders are affirmatively included in these longer decision- making processes.

(6.) FORMAT OPTIONS p. 55997

The NPRM notes two primary functional models using a variety of format options, the human decision variants and the computer decision variants. We see the human decision variant as described in the NPRM as a helpful "stopgap" measure during a transitional time from paper to electronically adjudicated claims. Even though the human decision variant represents a transitional process, the reality of HIPAA implementation is that even decades from now some providers may still be using the human decision variant. For this reason, it is important to pay attention to all details of the transitional system, which we have commented on in more detail below.

D. ELECTRONIC HEALTH CARE CLAIMS ATTACHMENTS BUSINESS USE p. 55998

(2.) SOLICITED VS. UNSOLICITED ATTACHMENTS p. 55999

We agree with HHS's decision to restrict unsolicited attachments, and to require solicited attachments insofar as this supports the minimum necessary standard and eases challenges with document storage, retrieval, and handling. However, we are concerned about the proposal to allow for the solicitation of only one attachment. The NPRM states:

> "We also propose that for each specific claim, health plans may solicit only one electronic attachment request transaction which would have to include all of their required or desired 'questions' and /or documentation needs relevant to that specific claim. Health care providers would be required to respond completely to the request, using one response transaction" (p. 55999).

We do not oppose the one-attachment policy as a policy matter. We are concerned about its privacy consequences. In order to comply with the one-attachment rule, it is probable that more data than is necessary will often be included in that attachment. Allowing only one solicitation may effectively reverse or undermine the minimum necessary standard.

Further, allowing a health provider to rely on a health plan's "request" as meeting the minimum necessary rule is problematic when taken together with the fact that only one solicitation will be allowable. We urge HHS to deny health care providers the ability to rely on health plan requests that are not consistent with the minimum necessary rule. The purpose is to ensure that the rule for one solicitation does not become a solicitation for all documentation in one fell swoop, even unnecessary documentation.

We recognize the inherent tension between providing for only one solicited attachment and asking that providers "consider" the minimum necessary rule. HHS needs to recognize that tension as well. We request HHS to articulate a way for providers to share information in that one solicited attachment in a way that respects privacy *and* the minimum necessary rule. HHS's commitment to privacy will be judged by how it resolves this tension. The need for a careful and privacy-protective resolution to this issue is magnified in importance by the fact that this is all a precursor to the NHIN, which will magnify the risks to privacy.

(4.) IMPACT OF THE PRIVACY RULE p. 55999

Reliance upon requestor should not apply in all circumstances

The NPRM allows a health care provider to rely upon a health plan's request for information as meeting the minimum necessary requirement:

> "A health care provider may rely, if such reliance is reasonable under the circumstances, on a health plan's request for information, or specific instructions for unsolicited attachments, as the minimum necessary for the intended disclosure" (p. 56000).

To the extent that a request is consistent with a standard or a practice within an industry, relying on a request appears to be readily acceptable. But – the reliance will

only be acceptable to the extent that a requester understands and complies with the minimum necessary standard. When a request goes beyond normal bounds, the ability to rely upon the request should no longer apply.

If health care providers are allowed to rely on a request to meet the standard, this leaves the door open to many abuses, particularly in the EDI environment. We request that HHS prohibit health care providers from relying upon requests that are not consistent with the minimum necessary rule. We understand that the NPRM gives providers the ability to retain the discretion to make their own minimum necessary determination, which is fine. However, the reliance loophole should be closed or narrowed.

Further, the policy allowing reliance runs the risk that industry practice will overwhelm the minimum necessary rule. If all insurers decide to insist on extraneous data elements, then the industry practice standard will mean that disclosure is acceptable even though the minimum necessary rule is not otherwise met. HHS needs to ensure that the creeping demands of administrative convenience do not overwhelm the intent of the minimum necessary policy.

Scanned documents and challenges to the minimum necessary rule

The NPRM states that in the case of submitting scanned documents, "efforts will be need to be made to ensure that those documents do not contain more than the minimum necessary information." When an attachment is sent as an image, adjudication will have to be accomplished manually using an image viewer or a web browser. Because this option represents the least organizational change in moving to electronically transmitted attachments, we expect that it will be a popular option. However, scanned documents represent a substantial challenge to the minimum necessary rule and pose many potential problems.

Providers do not always have the ability in the EDI environment to publish, or "print to electronic file" a medical file with precise control over specific content, as opposed to broad control over sections of a file. For example, a provider may need to submit the central medical data set to a health plan with an attachment. In a paper format, providers will frequently manually remove inapplicable pieces of paper in the central medical data set and attachments. By doing so, providers are able to comply with the

minimum necessary rule. However, when a provider has to "publish" a data set electronically (ie, create it in electronic format) , the provider may not be able to edit the content level of the data sets to a deep enough level in order to remove unnecessary data elements embedded within the data set. This is particularly true in the case of scanned documents, which may contain abundant data not connected to a claim.

Shortcomings of technology can undermine minimum necessary rule. We support HHS's efforts to continue application of the minimum necessary rule to scanned documents. We encourage HHS to broaden that rule to include all attachments.

(5.) Impact of the Security Rule p. 56000

We agree that all claims attachments must abide by the Security Rule, including scanned documents. We have concerns about the storage of attachments, particularly scans. We encourage HHS to consider long-term storage of attachments sent to health plans in any upcoming modifications to the Security Rule. This would include, for example, long term storage of attachments in databases.

(6.) Connection to Signatures p. 56000

The NPRM solicited input from industry on how "electronic signatures" should be handled when an attachment is requested and submitted electronically. The NPRM states in its discussion of "electronic signatures" that "a consensus standard does not presently exist that we could propose to adopt ..." (p. 56000). It is true that HHS could not adopt the current standard – which is a W3C standard -- due to HHS' restriction of adopting standards from only ANSI-accredited Standards Development Organizations specifically designated by HHS to manage the maintenance of the EDI standards adopted under HIPAA. [4] But there is nevertheless an industry consensus standard on (cryptographic) digital signatures. [5]

The W3C *xmldsig* is the widely recognized foundation for digital signatures. In

[4] ANSI is the acronym for the American National Standards Institute < http://www.ansi.org>; W3C is the World Wide Web Consortium < http://www.w3.org/Consortium/ >.

[5] We are using the term *digital signature(s)* to refer to cryptographic digital signatures. "Electronic signatures" can mean many things, including insecure, noncryptographic forms of signatures that would be inappropriate for use in handling healthcare claims attachments due to security vulnerabilities.

order to replicate a paper signature block, *xmldsig* is included in the schema and the bit of meta data in a traditional signature block is added. That is the way digital signatures are created and used currently. Reliance on this specification is nearly universal in XML messaging.

The W3C *xmldsig* is a consensus standard. The *xmldsig* is a W3C recommendation, which means it is approved by W3C members.[6] It has been incorporated into OASIS' WS-Security specification, which itself has been approved by OASIS' members, which has in turn been profiled by WS-I (in final stages of review). Whether something is taken up by WS-I and whether it is finally approved depends on what the organization calls an "N-1" consensus.

In its November 7, 2005 final rule, the Centers for Medicare and Medicaid Services adopted "foundation standards" for Medicare e-prescribing with its publication of its 42 CFR Part 423 Medicare Program; E-Prescribing and the Prescription Drug Program. The standards, which will be adopted January 1, 2006 include:

- Version 5.0 of the National Council for Prescription Drug Standards (NCPDP) Script standard, which allows physicians to transmit prescriptions to pharmacies;
- ASC X12N 270/271 Version 4010, which allows providers to check eligibility for benefits; and
- NCPDP Telecommunications Standard 5.1, which pharmacies can use to check eligibility.

Although the e-prescribing standards are officially adopted "foundation standards," these standards will not be adequate for use in healthcare claims attachments. Because the W3C *xmldsig* standard is already in use by large financial institutions and insurance companies, including in their use of attachments, it is entirely reasonable to expect that large commercial software vendors, as they write software to mesh billing and medical applications, will rely on the developed consensus standard in actual use, that is W3C *xmldsig*. If this happens on a wide scale, then hospitals, in order to use the software available to them, will likely use the defacto standard, *xmldsig*.

In light of its silence on digital signatures in electronic healthcare claims attachments, it is entirely possible that HHS will not be able to realistically change this

[6] See <http://www.w3.org/TR/xmldsig-core/>.

outcome. We foresee a possibility of HHS needing to adopt the W3C standard at a future date. On one hand, ignoring the standard may work, at least in the short term. But because W3C is not among the organizations designated to manage the maintenance of the EDI standards adopted under HIPAA, if the standard was eventually adopted, there may be some challenges.

Instead of ignoring the complex set of issues surrounding digital signatures, we urge HHS to find a reasonable way either to pilot test the existing W3C standard – and bring privacy stakeholders into that process – or to bring ASC X12N into the W3C process in a more robust way and find a way of making that process move faster and work more efficiently, or to employ a combination of the above. Because of rapid developments on adoption of digital signatures, it is unrealistic to expect that vendors will wait to build digital signatures into billing and other applications that hospitals can use until a standard is set by an HHS-designated ANSI-accredited standards organization.

We request that HHS face this issue head-on and work to incorporate the viewpoints of all stakeholders in the outcome.

G. PROPOSED STANDARDS p. 56004

In the general introduction to these comments, we discussed the challenges associated with adopting "industry consensus standards" as regulation without input from all stakeholder groups. It is difficult to come in at the late date of an NPRM and evaluate code sets for privacy and security considerations, much less effect any substantive change to enhance privacy and security at that point. We repeat our assertion that privacy stakeholders need to be involved in the standards making process, and that HHS require the standards bodies to show how they are working to involve privacy groups.

H. REQUIREMENTS p. 56012

I. SPECIFIC DOCUMENTS AND SOURCES p. 56013

VI. REGULATORY IMPACT ANALYSIS p. 56014

After the healthcare claims attachment rule is in effect for one year, we request that HHS prepare and make available to the public an analysis of the impact of this rulemaking on the privacy and security rule. HHS might ask the National Committee on Vital and Health Statistics to play a role in defining or conducting the analysis.

B. COSTS AND BENEFITS p. 56016

(4.) Cost and benefit estimates p. 56018

We question the HHS cost and benefit estimates. The specific estimates of cost savings from HIPAA transaction standards were, according to the NPRM, based on a single 1993 WEDI report coupled with "conservative assumptions" from the Transaction rule to predict costs and savings. The NPRM further states that some of the cost estimates were based on "informal discussions with industry representatives of health plans and vendors." A grouping of 12-year old data, "conservative assumptions," and informal discussions with industry members is not an appropriate factual basis upon which to rest either a broad assertion of cost saving or specific costs and savings assumptions.

Further, it is strange that the NPRM did not take into account the landmark WEDI/HL7/X12/AFEHCT National Healthcare Claims Attachment Survey Final Report in its proposed rulemaking. This report was published August 19, 2005, which gave HHS enough time to correct or at least inform some of the foundational errors in its calculations.

HHS relied upon the 1993 WEDI figure that 25 percent of all health care claims required support by an attachment or additional documentation. This figure has changed, as documented by the 2005 WEDI report. In the August 2005 WEDI report, the majority of health plan respondents surveyed stated that only 1 to 5 percent of claims required attachments. The next largest group of respondents stated that only 5 to 10 percent of claims required attachments (WETA 2005 Survey, p. 39). These numbers, if used, along with others, would have provided different cost and savings outcomes.

To begin to document and provide realistic and fact-based cost and savings analysis in this area, we request that HHS prepare and publish a sector-wide study to

determine actual costs and actual savings of the implementation of the healthcare claims attachments rule prior to promulgating the final rule. It is important to accurately determine costs and savings in the electronic environment, given the HHS focus on transitioning to an EDI-based process in many aspects of healthcare data collections and flows.

III. Conclusion

A recent national consumer survey found that "[C]onsumers continue to have serious misgivings about the security of their personal health information. Without strong safeguards, reliable privacy protection, and vigilant enforcement of privacy laws, public support for the national effort to develop a health care network could be in jeopardy" (National Consumer Health Privacy Survey 2005, California Health Care Foundation, November 2005, p. 2).

This conclusion is based in part on the response of 67 percent of 2100 people surveyed who stated they were "'somewhat' or 'very concerned' about the privacy of their personal medical records. In addition, the survey found that recent high-profile information privacy breaches have contributed to both the public's level of awareness about how much of their personal information is held by entities over which they have no control and how vulnerable that information is. This in turn has increased public concern about the privacy of medical records.

The adoption of standards for health claims attachments does not grab as many headlines as, for example, the NHIN. However, the health claims attachments standards will be widely used and will substantially impact patients' privacy. HHS must protect patient privacy, choice, and security in this process by maintaining the integrity of the minimum necessary standard in spirit and in practice, making the standards process more inclusive and fair, and generally balancing goals of EDI adoption with privacy. How HHS balances its goals of efficiency with protecting patient choice, privacy, and security will be an important test of how it will handle other issues such as the NHIN. The outcome will ultimately help or hurt patients' trust in the privacy of their medical records.

Respectfully submitted,

Pam Dixon
Executive Director
World Privacy Forum

and

Lee Tien
Senior Staff Attorney
Electronic Frontier Foundation

Melissa Ngo
Staff Counsel
Electronic Privacy Information Center

Linda Ackerman
Staff Counsel
PrivacyActivism

Beth Givens
Director
Privacy Rights Clearinghouse

Ed Mierzwinski
Consumer Program Director
U.S. Public Interest Research Group (U.S. PIRG), National Association of State PIRGs