Paper vs. Electronic
Records White Paper

SNIP

Paper vs. Electronic White Paper
Final Version – April 2003

SNIP Security and Privacy Workgroup

Workgroup for Electronic Data Interchange
12020 Sunrise Valley DR., Suite 100, Reston, VA. 20191
(t) 703-391-2716 / (f) 703-391-2759
© 2002/2003 Workgroup for Electronic Data Interchange, All Rights Reserved
Contents

Paper vs. Electronic................................................................. 1

Disclaimer.................................................................................. 1
Background.................................................................................. 1
Definition of the Medical Record................................................ 1
  Issues Associated with Paper Records and Electronic Records..... 2
  Characteristics of Electronic Medical Records.......................... 2
Security and Privacy of Transactions – Paper versus Electronic..... 3
Security and Privacy of Patient Records – Paper versus Electronic.. 3
National EMR Perspective............................................................. 4
  Long Term Benefits of EMR......................................................... 4
Ownership/Accountability............................................................. 4
Conclusion................................................................................... 5
Acknowledgements...................................................................... 5
Paper vs. Electronic

Disclaimer

This document is Copyright © 2002/2003 by The Workgroup for Electronic Data interchange (WEDI). It may be freely redistributed in its entirety provided that this copyright notice is not removed. It may not be sold for profit or used in commercial documents without the written permission of the copyright holder. This document is provided "as is" without any express or implied warranty.

While all information in this document is believed to be correct at the time of writing, this document is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult with an attorney. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by the Workgroup for Electronic Data Interchange. The listing of an organization does not imply any sort of endorsement and the Workgroup for Electronic Data Interchange takes no responsibility for the products, tools, and Internet sites listed.

The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by the Workgroup for Electronic Data Interchange (WEDI), or any of the individual workgroups or sub-workgroups of the Strategic National Implementation Process (SNIP).

Document is for Education and Awareness Use Only

The HIPAA Security and Privacy requirements are designed to be ubiquitous, technology neutral and scalable from the very largest of health plans, to the very smallest of provider practices. As the Privacy Rule and Security Rule relate to policies and procedures, many covered entities will find compliance not an application of exact template processes or documentation, but rather a remediation based on a host of complex factors unique to each organization.

Background

The final security and privacy rules for HIPAA implementation clearly state that both paper and electronic patient information are subject to the privacy provisions of the regulation but only electronic patient information is subject to the security provision of the regulation. The following information provides discussion and opinion on the current state of paper versus electronic medical records.

Definition of the Medical Record

One of the most important questions we need to address is what exactly is a patient medical record? The medical record appears to be a compilation of physician and nurse notes, with their opinions, suggestions and treatment options for an individual. Note: The medical record does not usually include the billing record, explanation of benefits etc. In addition to defining the actual medical record, other questions to be asked include:
• Why should the medical community invest in this entity?
• Shouldn’t it be the responsibility of the patients to chronicle their medical information themselves?
• Who are the primary users of the medical record?
• Who owns the medical record (information)?

Medical record documentation involves obtaining, displaying, compiling, retrieving, and analyzing data from various sources, and sharing the data both at the individual level but also at the organizational level. This information is used to assess and determined outcomes and is usually applied on a broad scale for entire population healthcare. In a technologically advance society the process of attempting to keep most of this vital information in our heads or on pieces of paper that can be misplaced or easily destroyed is dangerous and the move to electronic medical records should be encouraged.

The lack of widespread use of the electronic medical records (EMRs), otherwise known as Computerized Patient Records (CPR), has been one of the major difficulties in the development of standards that would allow for accurate collection of health information and data assessment. The EMR has been under siege recently due to the spotlight placed on the HIPAA regulations, especially in the privacy and security areas.

**Issues Associated with Paper Records and Electronic Records**

It is believed that that an improvement in the acquisition and analysis of data will occur with the use of EMR. The present challenge of paper-based records is that it creates a significant amount of inefficiencies. Paper based records are bulky, difficult to access and can only be used by one individual at a time. Entries in paper records are either hand written or typed, and therefore are prone to translation errors. The paper charts are transported manually from one location to the next. This practice allows for increased chance of security breach.

While all HIPAA covered entities must now safeguard administratively, physically, and technically the paper and electronic protected health information of patients, there remain drawbacks. Electronic medical records implementation is costly and the financial rewards are not always noticeable. There is no added reimbursable component to the healthcare provider for using EMRs. This is a cost that is borne only by the provider of care. It is believed that an improvement in the acquisition and analysis of data will occur with the use of EMR. Additionally, it is also believe that the overall efficiencies gained through the computerization of medical record will offset the cost of implementation.

**Characteristics of Electronic Medical Records**

Electronic information systems concentrate large amounts of data onto media that is generally stored in a centralized computer facility or machines. Security of the electronic data has three general components: administrative, physical and technical safeguarding.

Each covered entity should have analyzed and implemented policies and procedures dealing with administrative safeguards as part of implementation of the Privacy Final Rule.

Physical security of electronic data may be accomplished by maintaining servers or mainframe systems that house the data in a “locked and/or monitored” environment where access to the facility is restricted to authorized personnel only. The data needs to be backed-up regularly onto separate media that is stored in a separate, secure environment. Physical security of electronic data does not differ in many respects from that of paper-based data.
However, technical security for electronic data includes components that do not normally exist for patient information in a paper format. For example, data may be encrypted while being transmitted over telecommunications lines to prevent unauthorized access to patient information. In a paper system there is no clear equivalent to the type of unauthorized access that can occur in transmitting electronic data. Other aspects of logical security, such as restricting access to data by defining “rights” within the software, provide a level of security for electronic data that would be difficult to maintain in a paper system.

Security and Privacy of Transactions – Paper versus Electronic

Implementation of standards for transactions provides an excellent opportunity of converting from paper to electronic transactions since data content organization and format are the largest obstacles to performing electronic transactions. The overall intent of Administrative Simplification is to facilitate the use of electronic transactions to simplify and expedite administration of claims, reducing costs and improving healthcare delivery. While the cost of electronic systems may have provided a barrier to their implementation in the past, recent improvements in the availability of computers and telecommunications have effectively removed this barrier. Thus, it seems reasonable that all transactions (paper or electronic) should be held to the same standards for security and privacy.

Security and Privacy of Patient Records – Paper versus Electronic

Electronic patient records have distinct advantages over paper systems in regard to meeting both the security and privacy standards. Implemented using appropriate safeguards, electronic records systems have the advantage of providing improved access to records for physicians and the clinical support personnel, reducing clerical support costs, and facilitating the extract of “minimal necessary” data sets from records as needed. However, these systems provide significant challenges:

1. The most useful systems (meaning the systems providing best access to data via search functions) require physician data entry in a way that can significantly change the way physicians interact with patients. However these systems also provide electronic reminders about guidelines that can facilitate the healthcare process.

2. The software and hardware infrastructure of electronic patient information systems has a significant cost associated with both their implementation and maintenance. The success of such systems is largely dependent upon the upfront time and resources to correctly configure the system in order to have a positive outcome, along with the quality of ongoing support personnel and the computer skills of the personnel using the system.

3. For electronic systems determining the “ownership” of the data (for example, physician versus practice), the responsibilities of “stewardship” of the data (technical staff), and how and by whom access to data can be granted are key issues that impact significantly on security and privacy of the data. The popular belief that the record belongs to the patient is at odds with the necessity for physicians to fully document patient encounters and treatment plans for legal reasons as well as to support care delivery. The vision of providing a “lifetime” patient record that includes data from encounters with multiple physicians and multiple healthcare facilities may be limited to the “minimum necessary data” in a record “owned” by the patient.
4. Electronic systems rarely eliminate all paper elements of a record, but they do reduce the number of times paper records need to be handled.

In summary there are a variety of viewpoints on the issues around the cost, security and ownership of electronic medical records. The electronic patient information systems provide improved access to patient data, change the process of care delivery, and, if implemented correctly, improve the security and privacy of patient data. However, the cost of such systems must be weighed against the improved security and access. In order to provide access to a patient's data to another physician it would have to be indexed in a public system, stored, and secured so that transfer could occur to authorized users even if a different computer system were being used.

**National EMR Perspective**

To successfully provide a “lifetime” patient record that would be available to all healthcare providers for an individual patient the following factors seem to be required:

- A centralized, governmentally sponsored program that would set standards and host the system;
- Each patient would have a unique patient identification code (regulation not yet published);
- “Minimum necessary” data would be placed in the record by all physicians having encounters with the patient;
- The patient would “grant rights” to the physician to view and add data to their record as a condition for treatment; and
- The patient would always have view rights to the data and could ask for corrections to the record.

Because this would be the data shared with other physicians, there would be no need for a patient to ask for data to be changed in an individual physician’s private records. Physicians or practices that could not support an in-house electronic medical records system would only need a process to access the central system for viewing data and data entry; they could retain paper records at their practice site.

**Long Term Benefits of EMR**

The entire reason for the EMR is to realize efficiencies that would not be otherwise be realized. This concept is two fold. Initially the administrative savings (cost effectiveness) that are “promised” are the reason for the first step. The bigger picture is what the medical community can do with the information available (improvement on the health care delivery system itself). Alerts, reminders and other functions will initially help to lower utilization. Outcome modules (one day) will be able to intelligently assist physicians in determining the best procedure for a patient with a particular condition. Once again utilization will then decrease. The benefits gained from evaluating therapeutic interventions and measuring outcomes is seen not only at individual level, but also at the population level. This is one of the best reasons for nationwide implementation of EMRs.

**Ownership/Accountability**

Shouldn’t it be the responsibility of the patients to chronicle their medical information themselves? Who are the primary users of the medical record? Who owns the medical record (information)? Who should archive this documents/information and therefore bear the associated cost of archiving?
Accurate charting is a process of obtaining data, capturing data and analyzing this data to improve the diagnostic and therapeutic process. An EMR makes it easier for the patient to have an active role in both the content and the archiving of the information.

Implementation of an EMR is costly and the financial rewards are not always present at the individual provider level. Several healthcare provider organizations have implemented EMR systems at great cost, and found that it was not efficient and did not meet their needs. Some of these organizations have abandoned the EMR and will be reluctant to invest again in this costly enterprise. Other organizations have had wonderful experiences and are great supporters of the EMR. Alternatively other issues impact the response to the above question:

- Should the EMR be a public or private venture or a combination of both?
- Who should bear the cost?

In Europe with its socialized medicine, most of the cost of associated with the EMR is borne by the European Union. The European Union has invested several billion dollars into the development of EMRs.

**Conclusion**

Eventually, the EMR will provide more than a mechanism of protecting the access and privacy of the patient’s health information. In addition it will create a new and improved way of providing medical care. Lastly, the EMR will be used as a tool for accurate charting, appropriately obtaining data, and capturing and analyzing the data so that the information can be used to improve the process of diagnosis, therapeutic interventions and outcomes measures. The growth of medicine was highly linked to the advancement in the biological sciences during the 20th Century. This growth resulted in the development of disease control and therapies and pharmaceutical advances. The eventual benefit of the EMR will be the improvement in population health outcomes, the promotion of access to information while increasing protection and cost effectiveness of providing healthcare.

**Acknowledgements**

WEDI/SNIP would like to express its appreciation to the authors for their efforts in preparing this White Paper:

Maureen M. Levy, M.D., MBA  
Electronic versus Paper Sub-group Co-chair

Cleatus Wallis, Ph.D.  
Electronic versus Paper Sub-group Co-chair

J. Todd Preston  
**Final Version Edited by:**

Lesley Berkeyheiser  
The Clayton Group