SDFI®-TeleMedicine Security is Beyond HIPAA Security

When forensic examiners collect and capture digital evidence it must be protected from access beyond HIPAA. Not protecting forensic digital evidence beyond HIPPA can place a person in danger and result in a break in the chain of custody. Additionally, HIPAA does **NOT** apply to forensic exams because the act of providing a forensic exam is not an act of health care[(1)]. SDFI®-TeleMedicine is designed to protect forensic evidence beyond HIPAA.

- *Billing for a Forensic Exam*: Should the cost of a sexual assault forensic exam ever be processed under HIPAA rules, the suspect in the case could inadvertently be informed; thereby placing the alleged victim in danger before an investigation begins or concludes. For example, a child sexual abuse case where a suspect father controls the family's health care plan and receives a bill for the deductible related to the forensic exam [(2)].

- *Electronic Logs*: Any electronic log containing identifiable information could also expose an alleged victim to harm. Within a sexual assault program, an audit log can only serve to show who accessed the forensic record, after the fact, instead of safeguarding it upfront as SDFI does. Where audit logs record "past and previous" access, SDFI®-TeleMedicine prevents it.

- *The Federal Register:* The Federal Register, Vol. 68, Page 8336 states that, "It is possible that a small practice, with one or more individuals equally responsible for establishing and maintaining all automated patient records, will not need to establish policies and procedures for granting access to that electronic protected health information because the access rights are equal for all of the individual" [(3)]. This rule from the Federal Register specifically refers to patient health records, not forensic evidence or forensic evidence collection. SDFI-TeleMedicine security exceeds HIPAA security requirements.

- *The Federal Rules of Evidence:*[(4)] Article X, Rule 1002 states that: "An original writing, recording, or photograph is required in order to prove its content…" and in Rule 1001(d), "An 'original' of a photograph includes the negative...", the equivalent of a RAW file. Evidential photodocumentation must be protected beyond HIPAA. Only specially trained experts manage and handle forensic evidence ensuring a legal chain of custody. The Federal Rules of Evidence [(4)] also states that: "All laws in conflict with such rules shall be of no further force", superseding HIPAA Rules.

- *Protected Access to Forensic Evidence*: Within a sexual assault program, specially trained individuals are equally responsible for establishing and maintaining forensic evidence records. Unlike health records, only forensically trained professionals within the sexual assault program require access to the forensic evidence and information.

References:

1. http://www.sdfi.com/downloads/Forensic_Exams_and_HIPAA.pdf
2. http://archive.ahrq.gov/research/victsexual/victsex3.htm#Costs
3. http://www.gpo.gov/fdsys/search/submitcitation.action?publication=FR
4. http://www.uscourts.gov/RulesAndPolicies/rules/current-rules.aspx

Forensic Exams are NOT Covered Entities under HIPAA

Heath care means care, services or supplies related to the health of an individual.[1]

The purpose of a Sexual Assault Forensic Exam is to document exam findings and to collect, handle and preserve forensic evidence, not to provide health care. Health care, if offered, is be billed separately under HIPAA.

The Administrative Simplification Standards adopted by Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) only applies to an entity that is: [1]

- a health care provider that conducts certain transactions in electronic form.
- a health plan
- a health care clearinghouse

Forensic exams are not health care nor is a forensic exam covered under a health plan and payment for a forensic exam is not processed through a health care clearinghouse because it is not heath care. Forensic examiners and/or hospitals do not:

1. Furnish, bill, or receive payment for "health care or health care services" for forensic exam expenses.

   As a result of the Violence Against Women Reauthorization Act of 2013[2], states can no longer pay for exams by reimbursing the victim, instead they need to either provide the exams free of charge to the victim or arrange for victim to obtain the exams free of charge to the victims. Additionally, the state must incur the full out-of-pocket cost of the forensic exam, thus **the act of providing a forensic exam is not covered under HIPAA.**

2. Conducts covered transactions.

   In 45 CFR §162.1101[1][3], the Federal Register states that, *"The health care claims or equivalent encounter information transaction is the transmission of either of the following:*

   - *A request to obtain payment, and the necessary accompanying information* ***from a health care provider to a health plan, for health care.***

   - *If there is no direct claim, because the reimbursement contract is based on a mechanism other than charges or reimbursement rates for specific services, the transaction is the transmission of encounter information* ***for the purpose of reporting health care.****"*

   Forensic examiners and hospitals do not request payment from the victim or a victim's health plan, for forensic exams, nor do they utilize health care clearinghouses for payment or reimbursement for a forensic exam, thus **the act of providing a forensic exam is not covered under HIPAA.**

3. Transmit those transactions in electronic form.

   Evidence collected during a forensic exam is ***not transmitted for health care claim reasons or for health care,*** *thus* **the act of providing a forensic exam is not covered under HIPAA.**

If an entity does not meet the definition of a covered entity or business associate, it does not have to comply with the HIPAA Rules. [1]

References:

1). http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html
2). http://www.gpo.gov/fdsys/pkg/BILLS-113s47enr/pdf/BILLS-113s47enr.pdf
3). http://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-sec162-1101.pdf
4). http://www.sdfi.com/downloads/SDFI_is_Beyond_HIPAA_Security.pdf

Medical Examination and Treatment for Victims of Sexual Assault

Clinical Practice: Issues of Cost, Quality, and Access to Sexual Assault Services

The Agency's discussions with experts in the field pinpointed a number of issues in cost, quality and access to services for victims of sexual assault in urban, suburban and rural areas.

Costs Associated with Sexual Assault

There are few studies of the economic or medical costs associated with sexual assault, and little data on the use of medical services, either immediately, or over the long term. The studies that are available indicate that the long-term costs may be quite substantial in terms of ongoing visits to providers, missed work, and treatment for trauma (Rennison, 2002).

A 1996 NIJ Report (NIJ, 1996) supplements information obtained from the NCVS, which collects information only on short-term, out-of-pocket losses due to victimization. The NIJ report provides cost estimates for various types of violent crime that include longer range costs (e.g., those due to permanent disability and for mental health treatment) and intangibles such as pain, suffering, fear, and lost quality of life. The findings of the report include:

- Between 10 and 20 percent of mental health care expenditures in the U.S. may be attributable to crime victims who seek treatment as a result of their victimization. About half of these expenditures are for victims of child abuse who receive treatment as adults.
- Total costs per incident of non-fatal rape and sexual assault are estimated at $87,000, including $2,200 in productivity losses, $500 for medical care expenses, $2,200 for mental health care, and $81,400 associated with reduced quality of life.
- The average total cost per incident of child abuse is $60,000, including $2,200 in lost productivity, $430 in medical care costs, $2,500 for mental health care, and $52,371 in reduced quality of life. The greatest losses are associated with sexual abuse ($99,000 per incident), followed by physical abuse ($67,000) and emotional abuse ($27,000). (**Note:** The quality of life estimates were derived from the analysis of 1,106 jury awards and settlements to assault, rape and burn survivors to compensate for pain, suffering and lost quality of life [excluding punitive damages].)
- Total annual losses in the United States associated with child abuse (including sexual, physical, and emotional abuse) are estimated at $56 billion, including $23 billion specifically for rape and sexual assault.
- Total annual losses associated with rape and sexual assault of adults are estimated at $127 billion, including $4 billion in medical costs, $3.5 billion in other tangible costs, and $119 billion in quality of life.
- Total annual losses associated specifically with adult domestic violence (including fatalities, rape, other assaults and robbery) are estimated at $67 billion, including $1.8 billion for medical care, $7 billion for other tangible costs, and $58 billion for quality of life (these figures overlap substantially with those reported above for rape and sexual assault).

The 1995-96 NVAWS, a telephone sample survey that collected information on medical services provided to adult victims of rape, found that:

- About one-third (31 percent) of female rape victims reported physical injuries. Almost three-quarters of the injuries (73 percent) were minor (e.g., scratches, bruises or welts).
- About one third (36 percent) of those injured received some type of medical care. The majority of injured female victims who received care were treated in a hospital (82 percent). While most of those treated in a hospital were seen in the emergency room or an outpatient department, about 13 percent stayed for at least one night, with an average stay of 3.6

nights for those admitted on an inpatient basis.
- About half (55 percent) of all women who received medical care were treated by a physician outside of a hospital and averaged 4.8 office visits related to the injury. Somewhat less than a fifth received dental care (16.9 percent). A similar proportion visited a physical therapist (16.7 percent).

Return to Contents

Variations and Deficiencies in the Quality of Care

Among the issues identified with respect to quality of care and variations in practice are the following:

- **Lack of standardized protocols, procedures, and rape testing kits in use.** A number of protocols and procedures have been developed, but there is considerable overlap and many States end up reinventing well accepted standards. However, there remain important differences among the protocols in use and none have been compared or rigorously assessed. Even components which are fairly standardized have neither been systematically taught nor thoroughly evaluated.
- **A lack of trained providers and expert consultants.** There are curricula for teaching how to perform a medical evidentiary examination, but programs have reached only a few, self-selected providers (National Academy Press, 2002; Voelker, 1996). While there have been notable efforts by States to extend and support forensic training programs to health professionals already in practice, the sheer number and types of providers who may see a sexual assault victim is daunting. The IOM report, *Confronting Chronic Neglect* (National Academy Press, 2002) makes the point that all providers need basic competencies. Specific training needs will vary by profession, specialty and practice setting. In particular, special training and skills are required for addressing the needs of child victims as compared to adults.
- **Uneven quality of examination facilities and technologies available.** Most victims who seek medical care, though not all, are examined in a hospital setting. Many hospitals have developed special areas and separate facilities for examining patients, to provide a place where the lengthy examination will not impede care for other types of patients coming into an emergency room, to make available the special equipment and storage facilities used in such examinations, and to provide the victim a sanctuary that protects her or him from further traumatic experiences. Quiet, age-appropriate environments are thought to be especially important when examining children, who are particularly vulnerable to retraumatization and who also need examiners who are trained to meet the specialized needs of child victims. Specialized and separate sexual assault units within or near a hospital are viewed by many as ideal from a patient's perspective, but such facilities are not available in all hospitals. Reasons include lack of space; too few patients to make it an effective use of reserved space; an unwillingness or inability to spend the resources needed to establish and maintain a dedicated sexual assault unit; and a lack of understanding by administrators and/or the community about the importance of specialized care. Equipment and space are expensive resources, and smaller, rural hospitals may have particular difficulty creating a viable program, facility and trained staff.
- **Poor quality and limited capability to test for drugs and DNA.** Most hospitals do not routinely test for the full range of drugs (including substances used in drug-facilitated rape). Even fewer have the skills and technology to handle DNA testing, which has assumed additional importance with the advent of State DNA banks. DNA evidence can easily be compromised by untrained providers who are involved in the collection and preservation process. The sample can be contaminated if someone sneezes or coughs over the evidence, or even if the examiner touches his/her own hair or body and then touches the area to be tested. It is also affected by heat and humidity, and is easily degraded (Turman, 2001). Forensic DNA testing is a lengthy and expensive process, but one which is often paid for by the police department or prosecutor's office. However, even police labs often lack adequate forensic testing capabilities.

In partial response to these issues, a Federal law, the Paul Coverdell National Forensic Sciences Improvement Act, was enacted in 2000 (42 U.S.C. §§ 3797j et seq. (2002)). The Act authorizes about $500 million in Federal funds over a five-year period to be used by States to: improve procedures for testing DNA samples; hire and train personnel; modernize laboratory equipment; and improve the quality and timeliness of forensic science services.

Return to Contents

Access to Services

There are only sketchy descriptions available of the types and quality of services available to sexual assault victims. The reports available indicate wide variations in the types and quality of services received.

The NWS found that 55 percent of rape victims surveyed had not been given information on HIV testing and that one-third were not given information about other STD testing. The practice of immediate testing for STDs is controversial because any infection found would reflect prior exposure, and not all assaults will expose a patient to STD risks. However, others favor it as baseline information, and virtually all experts agree that the provider should stress the need for followup STD evaluation and treatment for patients at risk (CDC, 2002).

A 1996 survey of 130 Florida hospitals also provides a startling picture of the high degree of variation in services provided to sexual assault victims (Maxwell and Soubielle, 1996). Highlights of the findings from the 64 hospitals responding (49 percent) include:

- Most of the Florida hospitals surveyed (88 percent) saw rape victims through the emergency room.
- Some hospitals (six) reported that law enforcement personnel assist in the exam, a violation of the State's evidence collection protocol. Most experts in the field agree that, except in rare cases, there is no medical or legal reason for law enforcement representatives, male or female, to be present during the exam. Maintaining the chain of custody during the examination is a function and responsibility of the attending medical personnel and one that should not require outside assistance.
- Although the JCAHO requirements call for ongoing in-service training, only about one-fourth of hospitals reported that they provided such training for the personnel conducting examinations. (Information on followup activity initiated in response to findings about adherence to JCAHO requirements is not available.)
- Most hospitals only involve the local rape crisis center personnel if requested to do so by the victim, many of whom do not know that such services exist.
- Fewer than half of the hospitals reported that they provide written material on common rape reactions and community resources as a usual practice. Fifteen percent said they do not provide the victim with any information on resources.
- Just over half of the hospitals set aside separate rooms for rape victims and some provide showers for the rape victims after the exam, or maintain a clothing closet, or provide underwear or paper jump suits to patients whose clothing was collected.
- Most hospitals (82 percent) discussed HIV screening with patients and dispensed prophylactic drugs for sexually transmitted diseases (88 percent).

While interesting, these data, collected from 130 hospitals in Florida, may not be entirely reflective of national practices.

Access Issues Involving Payment for Evidentiary Exams

When a sexual assault victim presents to a hospital or clinic, medical staff will typically assess and respond to serious or life-threatening injuries. However, the decision to do a formal evidentiary examination is dependent on the patient who must give written consent, and is affected both by State laws and the judgment of local law enforcement officials or prosecutors as to whether an examination will be useful and can be justified.

Numerous Federal and State laws have been enacted to ensure that victims of sexual assault do not have to pay for medical evidentiary examinations. However, some States limit payment only to victims who are willing to report the assault to police and/or to cooperate in any prosecution. If the assault is not reported, or the case is not prosecuted, the victim may be unable to obtain a full examination, or may have to pay for the costs of an examination.

A number of States place responsibility for payment on the county where the sexual offense occurred, or on the entity who requests the examination, most often the investigating law enforcement agency or the prosecuting attorney. If the county official, police officer, or prosecutor is told that the victim does not plan to formally report the assault (a decision that the victim may not want or be able to make immediately, and a decision which sometimes changes), they may not approve payment for an examination. Similarly, if they believe that the victim's account is weak or that successful prosecution is unlikely, they may act to preserve limited resources and not provide approval for payment.

Even when State laws mandate that victims not be charged for the expense of evidentiary exams, there are cases in which claims may be submitted to third party insurance companies, compromising the victims' privacy, as insurance companies may not only be informed of the sexual assault but may also learn about exposure to HIV or other aspects of treatment that could affect insurance coverage in the future. Victims may also be forced to disclose the assault to the primary person on the insurance, such as a family member or even an employer.

Victims of crime are not generally required to cover the costs of evidence collection incurred in the investigation of their cases. Despite the fact that most States have laws that designate payment sources to cover the costs of forensic exams for sexual assault victims, and some even specifically prohibit billing of victims, billing of sexual assault victims continues to be widespread (National Center for Victims of Crime, 2003; National Center for Victims of Crime, 2001). Victims need to be informed of their rights and of avenues of recourse when rights are violated.

Return to Contents
Proceed to Next Section

Agency for Healthcare Research and Quality • 540 Gaither Road Rockville, MD 20850 • Telephone: (301) 427-1364

We received a number of comments that pertained to privacy issues. These issues were considered in the development of the Privacy Rule and many of these comments were addressed in the preamble of the Privacy Rule. Therefore, we are referring the reader to that document for a discussion of those issues.

2. Level of Detail

We solicited comments as to the level of detail expressed in the required implementation features; that is, we specifically wanted to know whether commenters believe the level of detail of any proposed requirement went beyond what is necessary or appropriate. We received numerous comments expressing the view that the security standards should not be overly prescriptive because the speed with which technology is evolving could make specific requirements obsolete and might in fact deter technological progress. We have accordingly written the final rule to frame the standards in terms that are as generic as possible and which, generally speaking, may be met through various approaches or technologies.

3. Implementation Specifications

In addition to adopting standards, this rule adopts implementation specifications that provide instructions for implementing those standards.

However, in some cases, the standard itself includes all the necessary instructions for implementation. In these instances, there may be no corresponding implementation specification for the standard specifically set forth in the regulations text. In those instances, the standards themselves also serve as the implementation specification. In other words, in those instances, we are adopting one set of instructions as both the standard and the implementation specification. The implementation specification would, accordingly, in those instances be required.

In this final rule, we adopt both ''required'' and ''addressable'' implementation specifications. We introduce the concept of ''addressable implementation specifications'' to provide covered entities additional flexibility with respect to compliance with the security standards.

In meeting standards that contain addressable implementation specifications, a covered entity will ultimately do one of the following: (a) Implement one or more of the addressable implementation specifications; (b) implement one or more alternative security measures; (c) implement a combination of both; or (d) not implement either an addressable implementation specification or an alternative security measure. In all cases, the covered entity must meet the standards, as explained below.

The entity must decide whether a given addressable implementation specification is a reasonable and appropriate security measure to apply within its particular security framework. This decision will depend on a variety of factors, such as, among others, the entity's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. Based upon this decision the following applies:

(a) If a given addressable implementation specification is determined to be reasonable and appropriate, the covered entity must implement it.

(b) If a given addressable implementation specification is determined to be an inappropriate and/or unreasonable security measure for the covered entity, but the standard cannot be met without implementation of an additional security safeguard, the covered entity may implement an alternate measure that accomplishes the same end as the addressable implementation specification. An entity that meets a given standard through alternative measures must document the decision not to implement the addressable implementation specification, the rationale behind that decision, and the alternative safeguard implemented to meet the standard. For example, the addressable implementation specification for the integrity standard calls for electronic mechanisms to corroborate that data have not been altered or destroyed in an unauthorized manner (see 45 CFR 164.312(c)(2)). In a small provider's office environment, it might well be unreasonable and inappropriate to make electronic copies of the data in question. Rather, it might well be more practical and afford a sufficient safeguard to make paper copies of the data.

(c) A covered entity may also decide that a given implementation specification is simply not applicable (that is, neither reasonable nor appropriate) to its situation and that the standard can be met without implementation of an alternative measure in place of the addressable implementation specification. In this scenario, the covered entity must document the decision not to implement the addressable specification, the rationale behind that decision, and how the standard is being met. For example, under the information access management standard, an access establishment and modification implementation specification reads: ''implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process'' (45 CFR 164.308(a)(4)(ii)(c)). It is possible that a small practice, with one or more individuals equally responsible for establishing and maintaining all automated patient records, will not need to establish policies and procedures for granting access to that electronic protected health information because the access rights are equal for all of the individuals.

a. *Comment:* A large number of commenters indicated that mandating 69 implementation features would result in a regulation that is too burdensome, intrusive, and difficult to implement. These commenters requested that the implementation features be made optional to meet the requirements. A number of other commenters requested that all implementation features be removed from the regulation.

Response: Deleting the implementation specifications would result in the standards being too general to understand, apply effectively, and enforce consistently. Moreover, a number of implementation specifications are so basic that no covered entity could effectively protect electronic protected health information without implementing them. We selected 13 of these mandatory implementation specifications based on (1) the expertise of Federal security experts and generally accepted industry practices and, (2) the recommendation for immediate implementation of certain technical and organizational practices and procedures described in Chapter 6 of *For The Record: Protecting Electronic Health Information,* a 1997 report by the National Research Council (NRC). These mandatory implementation specifications are referred to as required implementation specifications and are reflected in the NRC report's recommendations. Risk Analysis and Risk management are found in the NRC recommendation title System Assessment; Sanction Policy is required in the Sanctions recommendation; Information system Activity Review is discussed in Audit Trails; Response and Reporting circumstances.

In addition, a number of voluntary national and regional organizations have been formed to address HIPAA implementation issues and to facilitate

116TH CONGRESS
1st Session

COMMITTEE PRINT

No. 5

FEDERAL RULES

OF

EVIDENCE

DECEMBER 1, 2019

Printed for the use
of

THE COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

U.S. GOVERNMENT PUBLISHING OFFICE
WASHINGTON : 2020

AUTHORITY FOR PROMULGATION OF RULES

TITLE 28, UNITED STATES CODE

§ 2072. Rules of procedure and evidence; power to prescribe

(a) The Supreme Court shall have the power to prescribe general rules of practice and procedure and rules of evidence for cases in the United States district courts (including proceedings before magistrate judges thereof) and courts of appeals.

(b) Such rules shall not abridge, enlarge or modify any substantive right. All laws in conflict with such rules shall be of no further force or effect after such rules have taken effect.

(c) Such rules may define when a ruling of a district court is final for the purposes of appeal under section 1291 of this title.

(Added Pub. L. 100–702, title IV, § 401(a), Nov. 19, 1988, 102 Stat. 4648, eff. Dec. 1, 1988; amended Pub. L. 101–650, title III, §§ 315, 321, Dec. 1, 1990, 104 Stat. 5115, 5117.)

§ 2073. Rules of procedure and evidence; method of prescribing

(a)(1) The Judicial Conference shall prescribe and publish the procedures for the consideration of proposed rules under this section.

(2) The Judicial Conference may authorize the appointment of committees to assist the Conference by recommending rules to be prescribed under sections 2072 and 2075 of this title. Each such committee shall consist of members of the bench and the professional bar, and trial and appellate judges.

(b) The Judicial Conference shall authorize the appointment of a standing committee on rules of practice, procedure, and evidence under subsection (a) of this section. Such standing committee shall review each recommendation of any other committees so appointed and recommend to the Judicial Conference rules of practice, procedure, and evidence and such changes in rules proposed by a committee appointed under subsection (a)(2) of this section as may be necessary to maintain consistency and otherwise promote the interest of justice.

(c)(1) Each meeting for the transaction of business under this chapter by any committee appointed under this section shall be open to the public, except when the committee so meeting, in open session and with a majority present, determines that it is in the public interest that all or part of the remainder of the meeting on that day shall be closed to the public, and states the reason for so closing the meeting. Minutes of each meeting for the transaction of business under this chapter shall be maintained by the committee and made available to the public, except that any portion of such minutes, relating to a closed meeting and made available to the public, may contain such deletions as may be necessary to avoid frustrating the purposes of closing the meeting.

ARTICLE X. CONTENTS OF WRITINGS, RECORDINGS, AND PHOTOGRAPHS

Rule 1001. Definitions That Apply to This Article

In this article:

(a) A ''writing'' consists of letters, words, numbers, or their equivalent set down in any form.

(b) A ''recording'' consists of letters, words, numbers, or their equivalent recorded in any manner.

(c) A ''photograph'' means a photographic image or its equivalent stored in any form.

(d) An ''original'' of a writing or recording means the writing or recording itself or any counterpart intended to have the same effect by the person who executed or issued it. For electronically stored information, ''original'' means any printout—or other output readable by sight—if it accurately reflects the information. An ''original'' of a photograph includes the negative or a print from it.

(e) A ''duplicate'' means a counterpart produced by a mechanical, photographic, chemical, electronic, or other equivalent process or technique that accurately reproduces the original.

(As amended Apr. 26, 2011, eff. Dec. 1, 2011.)

Rule 1002. Requirement of the Original

An original writing, recording, or photograph is required in order to prove its content unless these rules or a federal statute provides otherwise.

(As amended Apr. 26, 2011, eff. Dec. 1, 2011.)

Rule 1003. Admissibility of Duplicates

A duplicate is admissible to the same extent as the original unless a genuine question is raised about the original's authenticity or the circumstances make it unfair to admit the duplicate.

(As amended Apr. 26, 2011, eff. Dec. 1, 2011.)

Rule 1004. Admissibility of Other Evidence of Content

An original is not required and other evidence of the content of a writing, recording, or photograph is admissible if:

(a) all the originals are lost or destroyed, and not by the proponent acting in bad faith;

(b) an original cannot be obtained by any available judicial process;

(c) the party against whom the original would be offered had control of the original; was at that time put on notice, by pleadings or otherwise, that the original would be a subject of proof at the trial or hearing; and fails to produce it at the trial or hearing; or

(d) the writing, recording, or photograph is not closely related to a controlling issue.

(As amended Mar. 2, 1987, eff. Oct. 1, 1987; Apr. 26, 2011, eff. Dec. 1, 2011.)

medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11).

(As amended Mar. 2, 1987, eff. Oct. 1, 1987; Apr. 25, 1988, eff. Nov. 1, 1988; Apr. 17, 2000, eff. Dec. 1, 2000; Apr. 26, 2011, eff. Dec. 1, 2011; Apr. 27, 2017, eff. Dec. 1, 2017.)

Rule 903. Subscribing Witness's Testimony

A subscribing witness's testimony is necessary to authenticate a writing only if required by the law of the jurisdiction that governs its validity.

(As amended Apr. 26, 2011, eff. Dec. 1, 2011.)

ARTICLE X. CONTENTS OF WRITINGS, RECORDINGS, AND PHOTOGRAPHS

Rule 1001. Definitions That Apply to This Article

In this article:

(a) A ''writing'' consists of letters, words, numbers, or their equivalent set down in any form.

(b) A ''recording'' consists of letters, words, numbers, or their equivalent recorded in any manner.

(c) A ''photograph'' means a photographic image or its equivalent stored in any form.

(d) An ''original'' of a writing or recording means the writing or recording itself or any counterpart intended to have the same effect by the person who executed or issued it. For electronically stored information, ''original'' means any printout—or other output readable by sight—if it accurately reflects the information. An ''original'' of a photograph includes the negative or a print from it.

(e) A ''duplicate'' means a counterpart produced by a mechanical, photographic, chemical, electronic, or other equivalent process or technique that accurately reproduces the original.

(As amended Apr. 26, 2011, eff. Dec. 1, 2011.)

Rule 1002. Requirement of the Original

An original writing, recording, or photograph is required in order to prove its content unless these rules or a federal statute provides otherwise.

(As amended Apr. 26, 2011, eff. Dec. 1, 2011.)

Rule 1003. Admissibility of Duplicates

A duplicate is admissible to the same extent as the original unless a genuine question is raised about the original's authenticity or the circumstances make it unfair to admit the duplicate.

(As amended Apr. 26, 2011, eff. Dec. 1, 2011.)

Rule 1004. Admissibility of Other Evidence of Content

An original is not required and other evidence of the content of a writing, recording, or photograph is admissible if: