

Confidentiality and Information Utilization

BACKGROUND

The confidential nature of communications between social workers and their clients has been a cardinal principle of the social work profession from its earliest years. Legislative protection for social work information in adoption and juvenile court records dates back half a century. The Social Security Act of 1935 (P.L. 74-271), as amended in 1939, required state public assistance plans to “provide safeguards which restrict the use or disclosure of information concerning applicants and recipients to purposes directly connected with the administration of [the program]” [Title IV, section 502(a) (8)]. The Office of Vocational Rehabilitation issued regulations during the 1940s requiring similar safeguards. There are specific federal statutes related to confidentiality of alcohol and drug treatment records (42 U.S.C. §§ 290dd-2; 42 C.F.R. pt. 2). In 1975, when special education became a federal mandate under the Education for All Handicapped Children Act of 1975 (P.L. 94-142), the first federal requirements concerning students with special needs and pupil records, including confidentiality and parental consent, were codified. These mandates were expanded under the Individuals with Disabilities Education Act (P.L. 90-247) and were reauthorized under the Individuals with Disabilities Education Act Amendments of 1997 (P.L. 105-17). With the advent of the HIV/AIDS epidemic, many states have enacted statutes protecting the confidentiality of an individual’s HIV/AIDS records and providing civil and criminal penalties for unlawful release of information (see, for example, N.J. Stat. 26: 5C-7, et seq., 2011). The Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191) (HIPAA) was enacted by the U.S. Congress, and it included administrative simplification provisions for streamlining the payment processes for

health care services. These included the creation of national minimum standards to secure confidentiality in the utilization of health care information. State and federal legislation, regulations, and guidelines dealing with a broad array of health, welfare, and educational programs in varying degrees have recognized the need for limiting and safeguarding the collection and use of personal data.

Social workers have access to clients’ personal information that is both confidential and privileged. Social workers are duty bound to protect all client information, regardless of the means by which it was conveyed. Issues of confidentiality and privacy are even more important now that the patient’s or client’s record—which once consisted of writing on pieces of paper—may consist of thousands of electronic bits of information that include written, audio, and visual records and links to other files within an agency or to other locations and may also include personal, medical, financial, and other types of data. Social workers are now using technology for documentation, electronic billing, communication, supervision, and client-based counseling. The NASW (2008) *Code of Ethics* provides strict guidelines for protection of confidentiality, informed consent, and maintenance and security of records [see 1.07, 1.03, 1.08, 2.02, and 3.04(c, d)].

Furthermore, there is an increasing amount of interdisciplinary communication within social work practice. Collaboration can, however, raise direct or indirect confidentiality dilemmas. Problems involved in the use or misuse of individually identifiable information, privacy, confidentiality, and privileged communications have commanded increased attention in both the public and private sectors of U.S. society in recent years.

In *Jaffee v. Redmond* (1996), the U.S. Supreme Court recognized a social worker–client privilege in the federal court system, protecting the confidentiality of patient and client communications with licensed therapists. Some federal legislation specifies confidentiality requirements for federal programs (such as Veterans Administration facilities), other legislation contains requirements for programs that receive federal funding (such as substance abuse and education programs), and still other federal legislation specifies confidentiality requirements that states must include in their programs as a condition of receiving federal grants.

HIPAA had a compliance date for its privacy rule in 2003, with detailed regulations about confidentiality and informed consent for an individual's health information (Centers for Medicare and Medicaid Services [CMS], 2010). HIPAA has standards for several areas that are pertinent to social work practice. These include using HIPAA-compliant computer billing software, ensuring the encryption of individually identifiable patient information that is electronically stored or transmitted, using secure passwords for protection of electronic data and electronic firewalls and physical safeguards for data backup in case of emergencies or natural disasters, maintaining an audit trail of access to electronic clinical information, and providing written notice to a client about privacy rights and how his or her information may be used (Morgan, Carvino, Polowy, & Kraft, 2007).

The Health Information Technology for Economic and Clinical Health Act (P.L. 111-5) (HITECH) was signed into law in 2009. This act promotes the use of electronic health records with the goal of making an electronic health record available for each person in the United States by 2014 (HITECH, 2009). HITECH also provides for increased privacy protection for personal health information and expands the scope of HIPAA to ensure that business associates providing services on behalf of health plans and health care providers are now directly subject to HIPAA regulations (Morgan & Polowy, 2009). HIPAA applies to clinical social workers, and it is important to note that the NASW *Code of Ethics* remains applicable as well in the area of electronic communications (Reamer, 2008).

In schools, hospitals, and agencies in which there is a team approach to treatment, disclosure of information frequently is critical to treatment planning and individualized educational programs. Insurance carriers and managed care firms often demand detailed diagnostic and other personal data in the name of accountability. Private practitioners and agency social workers are often subpoenaed to testify and reveal clients' confidences in divorce and custody proceedings and in other domestic lawsuits, and law enforcement agencies occasionally seek information from case records. In both public and private settings, social workers and other human services professionals must deal with the question of when legal protections of privacy—including statutory requirements for privileged communications—must yield to other legal requirements, such as protecting children from abuse or third parties from intended harm. When working collaboratively, social workers should ensure that colleagues understand social workers' obligations to respect confidentiality and any exceptions to it.

ISSUE STATEMENT

Over the past decade, the nation has seen the implementation of HIPAA and its expansion under the HITECH amendments, both of which have implications for social workers to uphold high standards for information use and release, data security and data storage, and how clients are informed about how personal data are being used (CMS, 2010; HITECH, 2009). With the increasing use of electronic communication and media of all formats in social work practice, these laws point to the importance of social workers maintaining the most current electronic security software to advance client confidentiality. These laws also discuss the importance of data destruction. Data destruction is an important area as the "complete" destruction of data takes specific intent; otherwise, data will remain on a system or electronic server, open to potential breach (Nelson, Phillips, & Steuart, 2010). Social workers need to be reminded of this technological fact to increase awareness about necessary steps to completely remove

electronic data from computers, networks, and other systems, including backup systems, to ensure client confidentiality.

Technological advances that have created the need for new regulations have also brought new ways to interact in virtual worlds and through social networking, with online chatting, Facebook, Skype, and even online counseling and virtual support groups. However, it is important to note that these platforms are not as secure and confidential as one might hope (Jones & Soltren, 2005). In fact, it has been reported that “over 40 percent of an individual’s [online] social ‘footprint’ can be reconstructed by using a single pseudonym” (Irani, Webb, Li, & Pu, 2009). Therefore, carefully setting passwords, restricting access to only authorized individuals, and thoughtfully posting online material helps to maintain client confidentiality as it helps to maintain professional boundaries for the social worker, much in the way that having an unlisted telephone number might have helped in the past.

The emergence and rapid expansion of information and communication technology have made the development of a strong information policy a primary concern for social workers. The social worker’s central role as the recipient and custodian of personal information places a particularly heavy responsibility on the social work profession and on individual practitioners to maintain current knowledge of legal requisites and then to weigh consequences, balance equities, and assume responsibility for actions taken. Social workers also bear a responsibility to understand the technologies used and to optimize the potential value of technology to serve clients effectively and efficiently while safeguarding against exposure of confidential information.

The profession also must reassess its policies and ethical base regarding privacy issues. It must consider the need to assume a more vigorous and active posture in this area, including the assumption of new advocacy roles. In addition, social workers must be aware of protections and constraints on patient or client confidentiality, which may be legally imposed. Every state has extended the protection of psychotherapist–patient privilege to communications with mental health professionals (*Jaffee v.*

Redmond, 1996), although what communications are protected and how professions are included varies (Polowy, Morgan, Bailey, & Gorenberg, 2008). Privilege may be waived by a patient or client, as the legally recognized holder of the privilege, or may be legally required to be breached, as in cases of child abuse or when it could prevent harm to a foreseeable victim. Privacy laws vary by state, and it is critical for social workers to be aware of these laws and changes in them. Some laws apply to the federal government—such as the Privacy Act of 1974 (P.L. 93-579), which makes unauthorized release a federal offense—and some federal laws apply to records in specific settings—such as the Family Educational Rights and Privacy Act of 1974 (P.L. 93-380), which protects the confidentiality of student records in schools and colleges that receive federal funding. The confidentiality of other records maintained by state and local governments may be protected by other statutes and regulations in specific locales.

In addition, social workers are constrained to some degree by privileged communication. Whereas confidentiality is a professional mandate, privileged communication is a legal issue in which a client’s right to privacy is protected by state or federal law. Many courts have held that the right belongs to the client and that only the client can waive the protection (NASW Legal Defense Fund, 2011; Polowy et al., 2008).

POLICY STATEMENT

NASW supports the following:

- Legislation, regulations, or policies that ensure adherence to the *NASW Code of Ethics* regarding confidentiality
- An individual’s right of access to personal information that is maintained about him or her and the right to decide how it is used
- An individual’s right to correct or amend a record of his or her identifiable information
- The profession becoming proficient in the technological tools and skills required for competent and ethical practice and staying current with emerging technology

- Information system technology that prevents unauthorized access to client information and *complete* record destruction in compliance with NASW & ASWB [Association of Social Work Boards] *Standards for Technology and Social Work Practice* (NASW & ASWB, 2005)
- Policies and practices that promote respect for confidential information exchanged by colleagues in the course of their professional relationships and transactions when collaboration is required and appropriate
- Social workers being fully knowledgeable about and compliant with federal and state regulations regarding confidentiality and information utilization.

REFERENCES

- Centers for Medicare and Medicaid Services. (2010). *HIPAA general information*. Retrieved from <http://www.cms.gov/HIPAAGenInfo/>
- Education for All Handicapped Children Act of 1975, P.L. 94-142, 89 Stat. 773 (1975).
- Family Educational Rights and Privacy Act of 1974, P.L. 93-380, 88 Stat. 571 (1974).
- Health Information Technology for Economic and Clinical Health Act, P.L. 111-5, 123 Stat. 226, 467 (2009).
- Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, 110 Stat. 1936 (1996).
- Individuals with Disabilities Education Act, P.L. 90-247, 81 Stat. 804 (1968).
- Individuals with Disabilities Education Act Amendments of 1997, P.L. 105-17, 111 Stat. 37 (1997).
- Irani, D., Webb, S., Li, K., & Pu, C. (2009). Large online social footprints—An emerging threat. In *Proceedings of the 2009 International Conference on Computational Science and Engineering* (pp. 271–276). Washington, DC: IEEE Computer Society.
- Jaffee v. Redmond, 518 U.S. 1, 116 S. Ct. 1923, 135 L.Ed.2d 337 (1996).
- Jones, H., & Soltren, J. H. (2005). Facebook: Threats to privacy. Retrieved from <http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-805-ethics-and-the-law-on-the-electronic-frontier-fall-2005/projects/facebook.pdf>
- Morgan, S., Carvino, L., Polowy, C. I., & Kraft, E. G. (2007). *The social worker and protection of privacy*. Washington, DC: NASW Legal Defense Fund.
- Morgan, S., & Polowy, C. I. (2009). *HITECH HIPAA for social workers*. Retrieved from https://www.socialworkers.org/ldf/legal_issue/2009/200903.asp
- NASW Legal Defense Fund. (2011). *Client confidentiality and privileged communications*. Washington, DC: NASW Press.
- National Association of Social Workers. (2008). *Code of ethics of the National Association of Social Workers*. Retrieved from <http://www.socialworkers.org/pubs/code>
- National Association of Social Workers & Association of Social Work Boards. (2005). *NASW & ASWB standards for technology and social work practice*. Retrieved from <http://www.socialworkers.org/practice/standards/NASWTechnologyStandards.pdf>
- Nelson, B., Phillips, A., & Steuart, C. (2010). *Guide to computer forensics and investigations*. Boston: Course Technology PTR.
- Polowy, C. I., Morgan, S., Bailey, W. D., & Gorenberg, C. (2008). Confidentiality and privileged communication. In T. Mizrahi & L. E. Davis (Eds.), *Encyclopedia of social work* (20th ed., Vol. 1, pp. 408–414). Washington, DC, and New York: NASW Press & Oxford University Press.
- Privacy Act of 1974, P.L. 93-579, 88 Stat. 1896 (1974).
- Reamer, F. (2008). The challenge of electronic communication. *Social Work Today*, 8. Retrieved from <http://www.socialworktoday.com/archive/EoEMayJun08.shtml>
- Social Security Act of 1935, P.L. 74-271, 49 Stat. 620 (1935).

NASW Members with Primary Responsibility for Revision of This Policy

First Draft Revision:

Raelene Freitag (WI)

Policy Panelists:

Brenda Pitmon (MA)
Patricia Findley (NJ)
Bettye Bradshaw (FL)
Elena Delavega (TX)
Kimiko Kuroda (CA)
Diana Stroud (IL)

Policy statement approved by the NASW Delegate Assembly, August 2011. This policy statement supersedes the policy statement on Confidentiality and Information Utilization approved by the Delegate Assembly in 2002. For further information, contact the National Association of Social Workers, 750 First Street, NE, Suite 700, Washington, DC 20002-4241. Telephone: 202-408-8600; e-mail: press@naswdc.org