

WEDI SNIP

Security and Privacy Workgroup Mission and Scope

Mission

As the health care community begins to implement the HIPAA security and privacy requirements, we must consider a national approach to the implementation of such requirements. As an industry we need to move forward in unison with the same understanding and goals. Otherwise, we are likely to experience a very difficult implementation, one fraught with confusion among the various constituencies. WEDI has undertaken the mission to develop a national, integrated approach that will enable the unified implementation of the HIPAA security and privacy requirements.

WEDI has created the Strategic National Implementation Process (SNIP) to address concerns being raised in the health care community by various organizations. SNIP is reviewing these issues, and others as they are identified, in order to recommend how we should move forward with the implementation in an orderly and efficient way.

SNIP is collecting information on current implementation projects and HIPAA training sessions and posting them to the WEDI SNIP web site at www.wedi.org/snip. SNIP is not going to reinvent the wheel if someone is already in the throws of the work. SNIP is cooperating and will loudly proclaim other efforts. SNIP is researching, outreaching, and writing white papers dedicated to areas of interest to the health care community.

WEDI SNIP holds periodic meetings in different parts of the country to update stakeholders on SNIP readiness work, educate on implementation strategies, receive input from interested parties and update the timeline.

Scope

The SNIP Security and Privacy Work Group has two distinct but related areas of Security and Privacy to review and provide implementation assistance information. The two areas have previously been developed separately as WEDI Policy Advisory Groups (PAGs) for policy discussion, outline and comment writing.

Since covered entities will need to implement both the security and privacy requirements at the same time, and most likely with the same planning and implementing team, it is logical to have both sets of HIPAA requirements reviewed by the same SNIP Work Group.

Security is the structure erected to protect the individual health information. Many of the requirements from the security standards either match the privacy standards, or flow one to another:

- The policies and procedures required in the security standards, and the policies and procedures necessary for the privacy standards both cover the same or similar areas.
- The new contract language for Business Associate Agreements within the security and privacy standards are related and the health care community will need to know the impact and barriers within each as they counter one another.

- When discussing the minimum necessary area of privacy one needs to understand the technical and manual security structure(s) capable of assisting in minimum necessary including policies and procedures.
- Within the security standards there are audit trails requirements, and the privacy standards anticipate expanded audit/accountability trails.
- When planning security awareness and education one must consider what patient information is being secured and protected.

Security is the “how,” privacy is the “what” and often the “why.”

Methodology

The Security and Privacy Work Group began working on five security implementation areas after the initial SNIP national meetings in June 2000. To date we have seven white papers in final form and seven under revision. We also will undertake a number of new white papers to address concerns arising from the recently issued Security Final Rule.

The white papers are posted to <http://www.wedi.org/snip/public/articles/index%7E10.htm>.

October 23, 2003