

RED FLAGS IDENTITY THEFT PREVENTION PROGRAM

Because they are likely to meet the Red Flags Rule's broad definition of "creditor" and have patient accounts that fall within the scope of "covered account," hospitals must develop a written identity theft prevention program. The FTC recently announced that it will *suspend enforcement* of the rule until May 1, 2009 to give hospitals and other organizations that are subject to FTC's regulatory oversight additional time to develop and implement their programs. However, the compliance deadline remains November 1, 2008 and hospitals should make a good faith effort to be in compliance with the rule's requirements as soon as possible.

To get hospitals started in developing their written identity theft programs, the AHA in cooperation with its outside counsel Hogan & Hartson LLP developed a sample policy that hospitals can use as a first step in developing and implementing a program that is responsive to the specific operations and needs of their individual organizations.

The final regulations state that an identity theft program "must be appropriate to the size and complexity of the [covered entity] and the nature and scope of its activities." ***While it may be appropriate to start with a sample policy, each organization must adapt the sample document to address the specific risks to their patient and other covered accounts and to ensure an appropriate and reasonable response to those risks.***

The sample policy is not intended to, and cannot, substitute for responsible legal advice. Hospitals should examine the sample document as part of a comprehensive risk assessment. Hospitals already may have processes and procedures in place to detect and respond to cases of potential identity theft and they will want to incorporate these existing activities into their individual organization's policy. Additionally, suggested guidelines for developing and structuring an identity theft program are included in the final rule's Appendix A, which starts on page 63773, and the supplement to the appendix identifies 26 potential red flags. While not all of the guidelines or red flags may be directly applicable to health care organizations, hospitals, *as the FTC has specifically urged*, should carefully consider and evaluate whether and how to incorporate them into their organization's policies and identity theft programs.

Hospitals also should carefully consider how compliance with other current federal and state legal requirements may impact the organization's identity theft policy. For example, EMTALA's obligations to provide without delay medical screening and stabilizing treatment for emergency medical conditions may affect policies related to verification of patient identity in the emergency department. HIPAA's privacy requirements will affect the design of policies that involve access to and sharing of patient information. State law security breach notification requirements may determine the reasonable response to an identified red flag.

The rule requires that organizations periodically reassess and revise their policies and practices, including modifications and/or expansions to detect and respond to new and

emerging risks. Hospitals will want to specifically charge someone within the organization with responsibility for maintaining and updating the program and policies and include such effort as an explicit component of the program from the start.