

ATTORNEYS:

Jeffrey P. Clark  
Mark A. Cameli  
John J. Lott  
Claudia J. Egan  
Shanti A. Ariker  
Daryll J. Neuser  
Meg S. L. Pekarske  
Lucien A. Beaudry  
Martin A. Machtan

1000 North Water Street  
P.O. Box 2965  
Milwaukee, Wisconsin  
53201-2965  
414-298-1000  
800-553-6215

22 East Mifflin Street  
P.O. Box 2018  
Madison, Wisconsin  
53701-2018  
608-229-2200  
800-728-6239

W233 N2080  
Ridgeview Parkway  
P.O. Box 2265  
Waukesha, Wisconsin  
53187-2265  
262-951-4500  
800-928-5529

## Crisis Management and Business Continuity News

Electronic Volume 2 • Issue 1 • 3/05/03

### HHS PUBLISHES FINAL ELECTRONIC INFORMATION SECURITY RULE

On February 20, 2003, the Department of Health and Human Services (HHS) published a final rule in the Federal Register adopting security standards for protecting individually identifiable health information when it is maintained or transmitted electronically. Under the Security Rule, most health care providers, health plans (including self-insured employers) and third parties providing services to these "covered entities" (such as billing services, accounting services, data processing and staffing services) must:

1. Ensure the confidentiality, integrity and availability of all electronic protected health information the covered entity creates, receives, maintains or transmits.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Security Rule.
4. Ensure compliance with the Security Rule by its workforce.

Compliance with the Security Rule begins with a two-step mandated process. Step 1: Assess the security risks. Step 2: Implement countermeasures proportional to those risks that stay current with new and increased risks.

The covered entity must implement certain safeguards, "standards" that describe the risk, and "implementation specifications" that describe the countermeasures. Each implementation specification is either "required" or "addressable". Addressable specifications must be met if the countermeasure is reasonable for a particular risk. The following "Security Standards Matrix" lists most of the standards, their implementation specifications and whether the specification is required or addressable:

Physical safeguards are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion.

#### PHYSICAL SAFEGUARDS

| Standards                           | Sections      | Implementation Specifications<br>(R)=Required, (A)=Addressable |     |
|-------------------------------------|---------------|--|-----|
| Facility Access controls<br><br>(A) | 164.310(a)(1) | Contingency Operations   | (A) |
|                                     |               | Facility Security Plan   | (A) |
|                                     |               | Access Control and Validation Procedures                       |     |
|                                     |               |  |     |
|                                     |               | Maintenance Records  | (A) |
| Workstation Use                     | 164.310(b)    |  | (R) |
| Workstation Security                | 164.610(c)    |  | (R) |
| Device and Media Controls           | 164.310(d)(1) | Disposal   | (R) |
|                                     |               | Media Re-use   | (R) |
|                                     |               | Accountability   | (A) |
|                                     |               | Data Backup and Storage  | (A) |

Technical safeguards mean the technology, policies and procedures that protect electronic protected health information and control access to it.

#### TECHNICAL SAFEGUARDS

| Standards             | Sections      | Implementation Specifications<br>(R)=Required, (A)=Addressable    |     |
|-----------------------|---------------|---|-----|
| Access control        | 164.312(a)(1) | Unique User Identification  | (R) |
|                       |               | Emergency Access Procedure  | (R) |
|                       |               | Automatic Logoff  | (A) |
|                       |               | Encryption and Decryption   | (A) |
| Audit Controls        | 164.312(b)    |   | (R) |
| Integrity             | 164.312(c)(1) | Mechanism to Authenticate Electronic Protected Health Information | (A) |
| Person or Entity      |               |   |     |
| Authentication        | 164.312(d)    |   | (R) |
| Transmission Security | 164.312(e)(1) | Integrity Controls  | (A) |
|                       |               | Encryption  | (A) |

Administrative safeguards are administrative actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

| ADMINISTRATIVE SAFEGUARDS |               |   |
|---------------------------|---------------|---|
| Standards                 | Sections      | Implementation Specifications             |
|                           |               | (R)=Required, (A)=Addressable             |
| Security Management       |               |   |
| Process                   | 164.308(a)(1) | Risk Analysis (R)                         |
|                           |               | Risk Management (R)                       |
|                           |               | Sanction Policy                           |
| (R)                       |               | Information System Activity Review (R)    |
| Assigned Security         |               |   |
| Responsibility            | 164.308(a)(2) | (R)                                       |
| Workforce Security        | 164.308(a)(3) | Authorization and/or Supervision (A)      |
|                           |               | Workforce Clearance Procedure (A)         |
|                           |               | Termination Procedures (A)                |
| Information Access        |               |   |
| Management                | 164.308(a)(4) | Isolating Health care Clearinghouse       |
|                           |               | Function (R)                              |
|                           |               | Access Authorization (A)                  |
|                           |               | Access Establishment and Modification (A) |
| Security Awareness        |               |   |
| and Training              | 164.308(a)(5) | Security Reminders (A)                    |
|                           |               | Protection from Malicious Software (A)    |
|                           |               | Log-in Monitoring (A)                     |
|                           |               | Password Management (A)                   |
| Security Incident         |               |   |
| Procedures                | 164.308(a)(6) | Response and Reporting (R)                |
| Contingency Plan          | 164.308(a)(7) | Data Backup Plan (R)                      |
|                           |               | Disaster Recovery Plan (R)                |
|                           |               | Emergency Mode Operation Plan (R)         |
|                           |               | Testing and Revision Procedure (A)        |
|                           |               | Applications and Data Criticality         |
| Evaluation                | 164.308(a)(8) | Analysis (A)                              |
| Business Associate        |               | (R)                                       |
| Contracts and             |               |   |
| Other Arrangement         | 164.308(b)(1) | Written Contract or Other Arrangement (R) |

The Security Rule officially takes effect on April 21, 2005, but may have a more immediate impact. The HIPAA Privacy Rules go into effect on April 14, 2003, and require implementation of "appropriate administrative, technical and physical safeguards" for all protected health information. To determine "appropriate safeguards," it is best to look to the Security Rule now to determine the necessary protection of electronic health information.

*Crisis Management and Business Continuity E-Newsletter* is an electronic publication of the law firm of Reinhart Boerner Van Deuren s.c., and is prepared by attorneys on the firm's Crisis Management and Business Continuity Team. This publication is intended to afford timely notice to our clients and friends of current events in Crisis Management and Business Continuity and to provide general information about Crisis Management and Business Continuity issues. It is not intended, nor should it be used, as a substitute for specific legal advice regarding particular factual situations.

[SUBSCRIBE](#)  
[UNSUBSCRIBE](#)



Printer friendly version

Feel free to forward this e-mail to a colleague.



---

© Reinhart Boerner Van Deuren s.c. 2002  
All Rights Reserved

This communication may be considered advertising in some jurisdictions.