

**Your company  
name/logo, contact  
information here**

Text Box: Remove this text and type your message. Adjust the font size and style as you would any text in Word®. You may (1) adjust the box size or (2) delete the text box by: "left clicking", moving the cursor to the border until you see (1) circles to move sides, or (2) the four direction arrow symbol to delete the box. For more information, see the document *Formatting Checklist*.

## **e-Essentials: EC Knowledge and Assessment**

### **SECURITY**

#### **CHECKLIST APPLICATION NOTE**

##### **Application Tips For Checklists**

The accompanying checklist that will be distributed in your facility represents a broad summary of common issues. While considering whether to supplement the checklist with current issues at your facility, you may want to consider the following subjects:

##### **Security for Patients and Visitors**

How the organization works to ensure a secure environment, from arrival (walking, parking, bus, and other means) through departure, for example:

- . A secure environment for people, possessions, vehicles
- . Signage and other visual aids to minimize disorientation due to unfamiliarity and stress (e.g., ability to orient, to find alarm and information systems such as direction signs, maps)
- . Ability to identify employees and the organization's security staff through badges, uniforms or other means.
- . Efforts to minimize the risk of assault, robbery and car jacking/abduction
- . Separation of patients and visitors from emergency operations that include security concerns (lock down, fire, disaster, etc.)

##### **Security for Employees and Professional Staff**

In addition to those for patients and visitors:

- . Additional concerns about coming and going at off hours
- . Ability to recognize and challenge strangers
- . Ability to recognize, respond to potentially dangerous people and situations
- . Access to the facility (control procedures and when they will be in place)

##### **Alarms and Paged Code Names**

- . Ability to recognize
- . Ability to respond

If you have pediatric patients and are using a single abduction code for all ages, you may want to consider modifying the code to help identify the age or other characteristic of the patient. This can help avoid confusion (e.g., staff looking for a young child when the missing person is older). For example, some facilities use a code "amber" for pediatrics and "pink" for infants as an additional help.

##### **Information Security**

Meeting the challenge of information security (e.g., HIPAA security rules) requires integration of information security through software, hardware and physical security

measures. You may want to describe some of the physical security aspects for HIPAA compliance when distributing this checklist. While JCAHO treats this under other sections of the accreditation manuals (IM standards), there is a need for coordination and collaboration to ensure the success of the physical and information security efforts. An example can be found in the article *Function Over Form*, by Joel Rakow in the December 2004 issue of Security Management Online (see references).

HIPAA security is a complex issue. The risk assessment, mitigation, and other activities vary among organizations; it is not possible to provide specifics here.

### **Risk Assessment**

Risk assessment and prioritization of effort, financial and other resources became an important part of EC management with JCAHO's realization that resources are limited. We seek processes that help us identify needs and priorities and ways to measure a baseline and to monitor our ability to maintain acceptable performance or to measure improvement. Just as important, we need to be able to prioritize our efforts.

We provide examples to illustrate potential approaches. Please note that these are examples of processes, and not data applicable to your situation.

Figure 1, Average Response Time, provides an example of a performance measure and the ability to compare current performance with past experience. The same performance measures can be used to establish needs and priorities. Establishing priorities and selecting the optimum response to vulnerabilities are judgment calls that should be guided by a security professional but have input from a multidisciplinary group.

Figure 2, Security Risk Identification and Prioritization Worksheet enables the assignment of numerical values to the *severity* and *probability* of security events. The number of disturbance calls in the emergency department is one type of event that can be associated with documented probability. Other data can be obtained externally. The worksheet provides space to document the various data sources and helps remind us to look beyond our organization. Incidentally it also helps assure JCAHO compliance.

Multiplying these two values *severity* and *probability* provides a measure of *relative risk*. The table can be sorted to rank priorities based solely upon these two numbers. We can go a step further in assigning priorities for resources by recognizing that the organization can manage the risk. For example, reducing vulnerability through more rapid response or by stationing a security officer in the area. This is accomplished by adjusting for the level of *preparedness*, assigning and dividing by a numerical value and then sorting on the last column. Thus the priority for resources can be assessed through analysis of projected impact of the resources, or by a retrospective analysis of experience.

Figure 3, Security Sensitive Areas; Risk-Based Protective Measures demonstrates a way to document the selection of appropriate protective measures (such as stationing a security officer in the area). This table can be used independently, or in conjunction with the spreadsheet shown in Figure 2.

The purpose of the Security Sensitive Areas Risk-Based Protective Measures is twofold: First, if used alone it identifies areas that have the potential for a security incident and documents the rank assigned. Second, it documents the actions taken to address the risks. Figure 3 illustrates this dual function. The entries can be color coded: One color for well controlled risks, a second for those in progress and a third color to identify those requiring attention. Further, the Xs can be replaced by letters to communicate even more information.

Please remember, our examples are just that; one risk assessment does not apply to all organizations. Even off-site entities likely will require their own risk assessment.

## EMERGENCY AREAS – DISTURBANCE CALLS

MONTH	AVERAGE CALLS	AVERAGE RESPONSE TIME (Minutes)
January	5	2.0
February	4	1.9
March	3	1.7
April	6	1.8
May	4	1.7
June	7	1.7
July	9	1.7
August	8	1.6
September	6	1.5
October	5	1.6
November	4	1.6
December	6	1.5
<b>Average</b>	<b>5.58</b>	<b>1.6</b>

Figure 1. The average response time recorded for the previous annual period was **2.9** minutes. The **1.6** minutes response time recorded in the immediate past year shows a 45% reduction in response time. Please note that the monthly average number of disturbance calls to the emergency areas is helpful in selecting the appropriate actions to address this vulnerability. By tracking and trending measurable data the organization can also seek external assistance through information sharing with colleagues, application of benchmarks and a search for best practices, and collaboration, both internal and external.

### Personalize This Checklist

Please personalize this checklist. Certain information (shown in red) commonly varies among facilities, and you may want to address other items.

### References

JCAHO, [www.jcaho.org](http://www.jcaho.org)

International Association for Healthcare Security and Safety, <http://www.iahss.org/>

ASIS International, Healthcare Security Council and Security Management Online  
<http://www.securitymanagement.com/>

American Health Information Management Association, <http://www.ahima.org/>

Rakow, J. Function Over Form. Security Management Online. December 3, 2004.  
<http://www.securitymanagement.com/library/001695.html>