Technical Committee on Health Care Emergency Management and Security (HEA-HES)

M E M O R A N D U M

DATE: July 25, 2012

TO: Principal and Alternate Members of the Technical Committee on Health Care Emergency Management and Security (HEA-HES)

FROM: Jon Hart, Associate Fire Protection Engineer/NFPA Staff Liaison

SUBJECT: **AGENDA PACKAGE– NFPA 99 First Draft Meeting (A2014)**

Enclosed is the agenda for the NFPA 99 First Draft meeting of the Technical Committee on Health Care Emergency Management and Security, which will be held on **Tuesday, August 14, 2012 and Wednesday, August 15, 2012 at the Sheraton Suites San Diego at Symphony Hall**. Please review the attached comments in advance, and if you have alternate suggestions, please come prepared with proposed language and respective substantiation.

If you have any questions prior to the meeting, please do not hesitate to contact me at:

Office: (617) 984-7470
Email: jhart@nfpa.org

For administrative questions, please contact Elena Carroll at (617) 984-7952.

I look forward to working with everyone.

Technical Committee on Health Care Emergency Management and Security (HEA-HES)

NFPA 99 First Draft Meeting (Annual 2014)

Tuesday, August 14, 2012 + Wednesday, August 15, 2012

Sheraton Suites San Diego at Symphony Hall

701 A Street, San Diego, California 92101

AGENDA

Tuesday, August 14, 2012 – Wednesday, August 15, 2012

1. Call to Order – 8:00 am (8/14)

2. Introductions and Attendanc**e**

3. Chairman Comments

4. Approval of Previous Meeting Minutes

5. Staff Liaison Presentation on NFPA's new Revision Process and A2014 Cycle

6. Review of Correlating Committee Minutes

7. Preparation of the First Draft
   - Review Public Input
   - Create First Revisions

8. New Business

9. Discuss dates for the TC Second Draft Meeting

10. Adjournment – (8/15)

Technical Committee on Health Care Emergency Management and Security (HEA-HES)

NFPA 99 First Draft Meeting (Annual 2014)

Tuesday, August 14, 2012 + Wednesday, August 15, 2012

Sheraton Suites San Diego at Symphony Hall

701 A Street, San Diego, California 92101

Key Dates for the Annual 2014 Revision Cycle

Public Input Closing Date	June 22, 2012
Final Date for First Draft Meeting	**August 31, 2012**
Ballots Mailed to TC before	October 12, 2012
Ballots Returned By	**November 2, 2011**
Correlating Committee First Draft Meeting	December 11, 2012
Final First Draft Posted	**February 22, 2013**
Public Comment Closing Date	May 3, 2013
Final Date for Second Draft Meeting	**July 12, 2013**
Correlating Committee Second Draft Meeting by	November 8, 2013
Final Second Draft Posted	January 3, 2014
Closing Date for Notice of Intent to Make a Motion (NITMAM)	February 7, 2014
Issuance of Consent Document (No NITMAMs)	*May 9, 2014*
NFPA Annual Meeting (Las Vegas)	June 2014
Issuance of Document with NITMAM	*August 12-14, 2014*

Technical Committee deadlines are in **bold**.

Technical Committee on Health Care Emergency Management and Security (HEA-HES)

NFPA 99 First Draft Meeting (Annual 2014)

Tuesday, August 14, 2012 + Wednesday, August 15, 2012

Sheraton Suites San Diego at Symphony Hall

701 A Street, San Diego, California 92101

Staff Liaison Notice

Note from the Staff Liaison

Dear Technical Committee Members:

We are very pleased that you will be participating in the processing of the 2015 Edition of NFPA 99, Health Care Facilities Code. Development of this document would not be possible without the participation of volunteers like you.

Meeting Preparation

Committee members are strongly encouraged to review the published comments prior to the meeting and to be prepared to act on each item.

Handout materials should be submitted to the chair and staff liaison at least seven days prior to the meeting.

Only one posting of the Public Input will be made; it will be arranged in section/order and will be pre-numbered. This will be posted to the NFPA 99 Document Information page (www.nfpa.org/99) under the "Next Edition" tab. If you have trouble accessing the website please contact Elena Carroll at ecarroll@nfpa.org.

Mandatory Materials:

- Last edition of the standard
- Meeting agenda
- Public Input
- Committee Officers' Guide (Chairs)
- Roberts' Rules of Order (Chairs; An abbreviated version may be found in the Committee Officer's Guide)

Optional Materials:

- NFPA Annual Directory
- NFPA Manual of Style

Technical Committee on Health Care Emergency Management and Security (HEA-HES)

NFPA 99 First Draft Meeting (Annual 2014)

Tuesday, August 14, 2012 + Wednesday, August 15, 2012

Sheraton Suites San Diego at Symphony Hall

701 A Street, San Diego, California 92101

Regulations and Guiding Documents

All committee members are expected to behave in accordance with the Guide for the Conduct of Participants in the NFPA Codes and Standards Development Process.

All actions during and following the committee meetings will be governed in accordance with the NFPA Regulations Governing Committee Projects. Failure to comply with these regulations could result in challenges to the standards-making process. A successful challenge on procedural grounds could prevent or delay publication of the document.

The style of the document must comply with the Manual of Style for NFPA Technical Committee Documents.

Distribution by %

HEA-HES Health Care Emergency Management and Security

Name	Company	Representation	Class	Office
William C. McPeck	State of Maine Employee Health & Safety		E	Principal
Tom Mayer Scheidel	Centers for Medicare and Medicaid Services		E	Principal
	Voting Number 2		**Percent** 13%	
Frank L. Keisler, Jr.	CNA Insurance Company		I	Principal
Michael D. Widdekind	Zurich Services Corporation		I	Principal
	Voting Number 2		**Percent** 13%	
James P. Simpson	National Joint Apprentice & Training Committee	IBEW	L	Principal
	Voting Number 1		**Percent** 6%	
Scott R. Fernhaber	Johnson Controls, Inc.		M	Principal
	Voting Number 1		**Percent** 6%	
Robert M. Becker	Incident Management Solutions, Inc.		SE	Principal
Jon M. Evenson	The RJA Group, Inc.	RJA	SE	Principal
Sharon S. Gilyeat	Koffel Associates, Inc.		SE	Principal
Jack Poole	Poole Fire Protection, Inc.		SE	Principal
Nicholas E. Gabriele	Russell Phillips & Associates, LLC		SE	Voting Alternate
	Voting Number 5		**Percent** 31%	
Susan B. McLaughlin	MSL Healthcare Consulting, Inc.	ASHE	U	Chair
Pete Brewster	US Department of Veterans Affairs	USVA	U	Principal
David A. Dagenais	Wentworth-Douglass Hospital		U	Principal
Steve Ennis	Virginia Hospital & Healthcare Association		U	Principal
Hulbert P. L. Silver	Central Newfoundland Regional Health Centre		U	Principal
	Voting Number 5		**Percent** 31%	
	Total Voting Number 16			

Address List No Phone

07/12/2012
Jonathan Hart
HEA-HES

Health Care Emergency Management and Security

Health Care Facilities

Susan B. McLaughlin **U** 1/15/1999
Chair **HEA-HES**
MSL Healthcare Consulting, Inc.
229 Whitney Drive
Barrington, IL 60010
American Society for Healthcare Engineering

Robert M. Becker **SE** 3/4/2008
Principal **HEA-HES**
Incident Management Solutions, Inc.
626 RXR Plaza
Uniondale, NY 11556
Alternate: Zachary Goldfarb

Pete Brewster **U** 10/28/2008
Principal **HEA-HES**
US Department of Veterans Affairs
Emergency Management Strategic Healthcare Group
510 Butler Avenue, Bldg. 203B
Martinsburg, WV 25405

David A. Dagenais **U** 1/25/2007
Principal **HEA-HES**
Wentworth-Douglass Hospital
789 Central Avenue
Dover, NH 03820

Steve Ennis **U** 4/16/1999
Principal **HEA-HES**
Virginia Hospital & Healthcare Association
14 Amara Drive
Fredericksburg, VA 22405

Jon M. Evenson **SE** 10/20/2010
Principal **HEA-HES**
The RJA Group, Inc.
Rolf Jensen & Associates, Inc.
600 West Fulton Street, Suite 500
Chicago, IL 60661-1241
Alternate: Richard A. Mahnke

Scott R. Fernhaber **M** 3/15/2007
Principal **HEA-HES**
Johnson Controls, Inc.
2400 Kilgust Road
Madison, WI 53713-4842

Sharon S. Gilyeat **SE** 1/25/2007
Principal **HEA-HES**
Koffel Associates, Inc.
8815 Centre Park Drive, Suite 200
Columbia, MD 21045-2107
Alternate: Jennifer L. Frecker

Frank L. Keisler, Jr. **I** 8/9/2011
Principal **HEA-HES**
CNA Insurance Company
425 Arborshade Trace
Duluth, GA 30097-8069

William C. McPeck **E** 7/1/1996
Principal **HEA-HES**
State of Maine Employee Health & Safety
PO Box 137
Saint Albans, ME 04971

Jack Poole **SE** 03/05/2012
Principal **HEA-HES**
Poole Fire Protection, Inc.
19910 West 161st Street
Olathe, KS 66062-2700

Tom Mayer Scheidel **E** 10/4/2007
Principal **HEA-HES**
Centers for Medicare and Medicaid Services
8805 Ridge Run Drive
North Richland Hills, TX 76180

Hulbert P. L. Silver **U** 03/05/2012
Principal **HEA-HES**
Central Newfoundland Regional Health Centre
22 Sunset Drive
Grand Falls-Windsor, NL A2A 1W7 Canada

James P. Simpson **L** 1/10/2008
Principal **HEA-HES**
National Joint Apprentice & Training Committee
17201 Sodium Street, NW
Ramsey, MN 55303-7313
International Brotherhood of Electrical Workers

Address List No Phone

07/12/2012
Jonathan Hart
HEA-HES

Health Care Emergency Management and Security

Health Care Facilities

Michael D. Widdekind **I** 1/14/2005

Principal **HEA-HES**
Zurich Services Corporation
Risk Engineering
112 Andrew Court
Centreville, MD 21617

Nicholas E. Gabriele **SE** 10/20/2010

Voting Alternate **HEA-HES**
Russell Phillips & Associates, LLC
31 Cooke Street
Plainville, CT 06062
Voting Alt. for Russ Phillips & Assoc.

Chad E. Beebe **U** 10/20/2010

Alternate **HEA-HES**
ASHE - AHA
PO Box 5756
Lacey, WA 98509-5756

Jennifer L. Frecker **SE** 10/28/2008

Alternate **HEA-HES**
Koffel Associates, Inc.
8815 Centre Park Drive, Suite 200
Columbia, MD 21045-2107
Principal: Sharon S. Gilyeat

Zachary Goldfarb **SE** 3/4/2008

Alternate **HEA-HES**
Incident Management Solutions, Inc.
626 RXR Plaza
Uniondale, NY 11555
Principal: Robert M. Becker

Richard A. Mahnke **SE** 3/2/2010

Alternate **HEA-HES**
The RJA Group, Inc.
Sako & Associates, Inc.
600 West Fulton Street, Suite 500
Chicago, IL 60661-1241
Principal: Jon M. Evenson

Jonathan Hart 3/1/2012

Staff Liaison **HEA-HES**
National Fire Protection Association
1 Batterymarch Park
Quincy, MA 02169-7471

TC on Emergency Management and Security
ROC Meeting
October 15, 2010
9:00 am EDT – 12:00 pm EDT
Windows Live

Attendees:

George Stevens
Zachery Goldfarb
Scott Fernhaber
David Dagenais
Russell Phillips
Michael Widdekind
Robert Becker
Sharon Gilyeat
Susan McLaughlin
William McPeck

Richard Bielen
Jon Levin

1. George Stevens called the meeting to order. He stated we have public comments to review for this meeting.

2. Jon Levin gave the staff report. He reviewed the dates of the cycle and the actions the committee can take at the ROC meeting.

3. The minutes of the previous ROP meeting were approved.

4. The committee then acted on the public and committee Comments. See the ROC for the official action on the comments.

5. There was no old business.

6. There was no new business.

7. Next meeting. TBD.

8. Meeting adjourned at 10:50 am.

99- Log #282 HEA-HES Final Action:
(12.5.3.3.8.4(2))

Submitter: Susan B. McLaughlin, MSL Healthcare Consulting, Inc.
Recommendation: Revise text to read:
(2) Assessment of ~~stand-alone capability~~ sustainability
Substantiation: The term "sustainability" is now commonly used in lieu of the term "stand-alone capability."

99- Log #283 HEA-HES Final Action:
(12.5.3.4.5.2)

Submitter: Susan B. McLaughlin, MSL Healthcare Consulting, Inc.
Recommendation: Revise text to read:
12.5.3.4.5.2 Prior to beginning work, ~~efforts shall be made to verify identities~~ the identity of other volunteers offering to assist during response activities must be verified.
Substantiation: Verification of the identity of non-clinical volunteers is mandatory. Previous wording could be interpreted that this is an optional activity.

99- Log #284 HEA-HES Final Action:
(12.5.3.6.1(3))

Submitter: Susan B. McLaughlin, MSL Healthcare Consulting, Inc.
Recommendation: Add new text to read:
(3) Updates to the facility emergency supplies inventory
Substantiation: The Joint Commission requires this third update as part of the annual evaluation process.

99- Log #64 HEA-HES Final Action:
(13.1)

Submitter: Michael D. DeVore, State Farm Insurance
Recommendation: Revise to read:
This chapter shall ~~provide those with the responsibility for security in new~~ apply to new and existing health care facilities ~~with the criteria to develop a security management program~~.
Substantiation: The existing sentence did not contain a requirement. The explanatory language was removed to the annex and the sentence revised to show the applicability of the chapter, which matches content in other chapters of NFPA 99.

99- Log #66 HEA-HES Final Action:
(13.1.1 and 13.1.2)

Submitter: Michael D. DeVore, State Farm Insurance
Recommendation: Delete as follows:
~~13.1.1* A health care facility shall have a security management plan.~~
~~13.1.2* The scope, objectives, performance, and effectiveness of the security plan shall be tested at a frequency shown to be necessary by review of the security vulnerability assessment (SVA) in accordance with Section 13.2.~~
Substantiation: Sections moved to 13.2 in public input #67.

99- Log #68 HEA-HES Final Action:
(13.2)

Submitter: Michael D. DeVore, State Farm Insurance
Recommendation: Revise to read:

13.2 Security ~~Vulnerability Assessment (SVA)~~ Plan.

13.2.1* A health care facility shall have a security management plan.

13.2.2 The health care facility shall conduct a security vulnerability assessment (SVA) as part of the security plan.

13.2.~~2~~3 The SVA shall evaluate the potential security risks posed by the physical and operational environment of the health care facility to all individuals in the facility.

13.2.~~3~~4 The facility shall implement procedures and controls in accordance with the risks identified by the SVA.

13.2.5 The scope, objectives, performance, and effectiveness of the security plan shall be tested at a frequency shown to be necessary by review of the security vulnerability assessment (SVA).

Substantiation: Reorganized sections under heading of Security Plan for clarity. Section 13.1.1 becomes 13.2.1 and section 13.1.2 becomes 13.2.5. The existing sections of 13.2 are renumbered. The security plan and plan evaluaton do not fit under Scope. The SVA is actually part of the SVA so all of this text should be together under the one heading.

99- Log #285 HEA-HES Final Action:
(13.3.2(o), (p), and (t))

Submitter: Susan B. McLaughlin, MSL Healthcare Consulting, Inc.
Recommendation: Revise text to read:

~~(o) Homeland Security advisory system (threat level changes)~~

(p) ~~Suspicious powder or substance~~ Suspicious package

(t) Active shooter

Substantiation: Removing Homeland Security threat level changes: Hospitals typically do not adapt policies to threat level changes. Change "suspicious powder or substance" to "suspicious package." Any suspicious powder or substance will likely be contained within a suspicious package, which hospital receiving departments should be trained to recognize.

Add Active Shooter policy: Given events that have taken place in hospitals, most are developing and implementing this policy.

99- Log #73 HEA-HES Final Action:
(13.4, 13.5, and 13.6 (New))

Submitter: Michael D. DeVore, State Farm Insurance
Recommendation: Add new sections to read:

13.4 People Management.
13.4.1 Employees.
13.4.1.1* Employers shall promote trustworthiness by using the following personnel practices for employees with access to critical assets:
(1)* Background screening
(2) Verification of background screening of contracted personnel acting in the capacity of employees
(3) Drug testing program
13.4.1.2* Identification badges shall have a photograph of the bearer and the bearer's name.
13.4.1.3 When identification badges are issued, employees shall, as indicated in the security plan, do one but not both of the following:
(1) Display the badge at all times
(2) Display the badge on demand
13.4.2 The Public. Public visitation controls shall be enforced.
13.4.2.1 After-hours entrance by the public shall be restricted to designated areas such as entrance lobbies and emergency departments.
13.4.2.2 Health care facility security controls and procedures shall comply with life safety requirements for egress.
13.4.3* The Media. The security management plan shall include procedures to accommodate media representatives.
13.4.3.1 A person shall be designated to serve as media contact and representative for the organization in regard to media interactions.
13.4.3.2 An area shall be designated for assembly of media representatives.
13.4.3.2.1 A security or facility staff member shall remain with the media representative(s) at all times.
13.4.3.2.2* Media representatives shall be escorted when granted access to the health care facility outside of the area designated in 13.4.3.2.
13.4.4* Crowd Control.
13.4.4.1 The security management plan shall provide procedures for crowd control demanding access to a health care facility.
13.4.4.2 The procedures for managing crowd control shall provide for coordination and collaboration of security and law enforcement.
13.4.5* Security Personnel.
13.4.5.1 Personnel Requirements.
13.4.5.1.1 The number of security personnel shall be determined by the security plan and the person responsible for facility security.
13.4.5.1.2 Selection criteria for security personnel shall include but not be limited to the following:
(1) Federal, state, and local laws and regulations
(2) Knowledge of criminal activities and proper law enforcement response procedures
(3) Good judgment and emotional stability
(4) Experience and demonstrated ability to retain composure under pressure
(5)* Disclosure of charges or convictions for felonies or crimes involving dishonesty or moral turpitude
13.4.5.2* Security Duties.
13.4.5.2.1 Facilities with security personnel shall have post orders.
13.4.5.2.2 Post orders shall contain instructions to cover reasonably foreseeable events security personnel may encounter.
13.4.5.2.2.1 Post orders shall list the name of the facility, the date issued, effective date, and purpose.
13.4.5.2.2.2 Post orders shall list security personnel duties, including but not be limited to the following:
(1) Authority of security personnel
(2) Emergency response procedures
(3) Job classification
(4) Uniforms
(5) Authorized weapons, including firearms, batons, and mace
(6) Reporting times

(7) Security patrols
(8) Hours of coverage
(9) Facility rules and regulations
(10) Applicable federal, state, and local laws
(11) Other duties to be assigned
13.4.5.2.2.3* Instructions shall be lawful and endeavor to protect the safety of security personnel and those they interact with in performance of their duties.
13.4.5.2.3 Post orders shall be reviewed and updated at a frequency shown to be necessary by review of the SVA.
13.4.5.2.3.1 Facility management and security management shall periodically assess post orders to identify and correct operational problems.
13.4.5.2.3.2 A procedure shall be established to inform security personnel of changes in post orders.
13.4.5.3* Supervision.
13.4.5.3.1* Security patrols shall be supervised.
13.4.5.3.2 Records shall be kept, including but not limited to the following:
(1) Crimes discovered by or reported to security personnel
(2) Frequency of patrols
(3) Activity log
(4)* Exceptions log
13.4.5.3.3 Security records shall be retained for not less than 5 years or until the expiration of the appropriate statute of limitations, whichever is longer.
13.4.5.4 Security Personnel Communications. Field security personnel shall have a process and means to communicate with a security office or public safety agencies.
13.4.5.5* Weapons and Equipment.
13.4.5.5.1 Security personnel shall carry only authorized equipment.
13.4.5.5.2 When weapons are authorized, policies and procedures governing their storage, handling, and use shall be established.
13.4.5.6* Training.
13.4.5.6.1 Security personnel shall be trained in the performance of their duties.
13.4.5.6.2 Security personnel that carry weapons shall be trained in their storage, handling, and use.
13.4.5.6.3 Armed security personnel shall have firearms training.
13.4.5.6.4 Security personnel in health care facilities should have additional training to include but not be limited to the following:
(1) Customer service
(2) Emergency procedures
(3) Patrol methods
(4) De-escalation training
(5) Use of physical restraints
(6) Use of force
13.5 Material Receiving.
13.5.1 Commercial Receivables.
13.5.1.1* Shipments coming into facilities shall be stopped for entry authorization and dock assignment.
13.5.1.1.1 Shipments coming in shall be expected and have corresponding purchase orders or requisitions.
13.5.1.1.2 Undocumented deliveries shall not be accepted.
13.5.1.2 Receipt of hazardous materials shall be documented and tracked.
13.5.2 Package Deliveries.
13.5.2.1 Packages being delivered shall be inspected for evidence of tampering or damage.
13.5.2.2* Any damaged or suspicious packages shall be reported to the carrier.
13.5.3 Mail.
13.5.3.1* Employees who handle mail shall evaluate the appearance of incoming packages to determine if they fit the characteristics of mail normally received.
13.5.3.2 The recipient of a letter or package shall evaluate the delivery to determine if a package is from an unknown, unsolicited source.
13.5.4 Couriers.
13.5.4.1 Couriers making deliveries shall provide identification.
13.5.4.2 Courier identification shall be entered into a delivery log or attached to the item being delivered.
13.6 Security Perimeters.
13.6.1 General.

13.6.1.1 The area covered by the security plan shall be defined by the security vulnerability assessment (SVA).
13.6.1.2* The primary security perimeter shall include the total area in the security plan.
13.6.1.3* Secondary security perimeters within the primary security perimeter shall be areas identified as either secured or unsecured.
13.6.1.4* Movement through every portal in a secured perimeter shall be controlled.
13.6.1.5 Physical barriers or security systems utilized or installed in security perimeters shall comply with applicable fire code or other life safety requirements.
13.6.2* Area Designations. Areas within secondary security perimeters should be designated as one of the following:
(1) Unsecured
(a) Open
(b)Protected
(2) Secured
(a) Controlled
(b) Restricted

Substantiation: The new text is from NFPA 730, 2011 edition. NFPA 730 went through a complete revision going into the 2011 edition. Each occupancy chapter was normalized in format. This additional language reflects the revisions to NFPA 730, chapter 12 on Healthcare.

99- Log #75 HEA-HES Final Action:
(13.4.1 through 13.4.8)

Submitter: Michael D. DeVore, State Farm Insurance
Recommendation: Revise to read:

13.46.3.1 ~~All security~~ Security-sensitive areas, as identified by the SVA, shall be ~~protected~~ classified as ~~appropriate~~ controlled or restricted.
13.46.3.2
13.46.3.3
13.46.3.4*
13.46.3.5
13.46.3.6
13.46.3.7
13.46.3.8

Substantiation: Renumber the section to match the proposal for additional text from NFPA 730, 2011 edition. Change the first paragraph to state that entrance to security-sensitive areas needs to be controlled and the control measures are determined by whether the area is controlled or secured. See the earlier public input for the classification of spaces in the security plan.

99- Log #77 HEA-HES Final Action:
(13.5)

Submitter: Michael D. DeVore, State Farm Insurance
Recommendation: Revise to read:

~~13.5 Access and Egress Security Measures.~~
~~13.5.1 Public visitation controls shall be enforced.~~
~~13.5.2 After-hours entrance by the public shall be restricted to designated areas, such as entrance lobbies and emergency departments.~~
~~13.5.3 Health care facility security controls and procedures shall comply with life safety requirements for egress.~~
~~13.5.3.1*~~ 6.4* Special Conditions. Security plans for health care occupancies shall address access and egress control during periods of quarantine and other events in conjunction with emergency agencies.

Substantiation: The deleted text is submitted in another public input to become new section 13.4.2. Numbering and title of the remaining section is revised for manual of style and to match the numbering in previous public inputs.

99- Log #81 HEA-HES Final Action:
(13.6, 13.7, 13.8, 13.9, and 13.10)

Submitter: Michael D. DeVore, State Farm Insurance
Recommendation: Delete all of 13.6, 13.7, 13.8, 13.9, and 13.10.
Substantiation: Delete this material because it was moved to people management and portal control sections as proposed in public inputs to reorganize Chapter 13 based on the complete revision of NFPA 730, in the 2011 edition.

99- Log #78 HEA-HES Final Action:
(13.7 (New))

Submitter: Michael D. DeVore, State Farm Insurance
Recommendation: Add a new section to read:
13.7 Portal Control.
13.7.1 General.
13.7.1.1 The number of portals in a security perimeter shall be restricted to the minimum required for safe and efficient operation of the facility.
13.7.1.2* Movement through portals in security perimeters shall be controlled.
13.7.2 Exterior Portals.
13.7.2.1 Exterior entrances shall be provided with locking devices.
13.7.2.2 Exterior hinge pins on doors in security perimeters shall be secured against removal.
13.7.3 Locks.
13.7.3.1* Egress and fire resistance provisions relating to doors and hardware shall be maintained.
13.7.3.2 Individual products shall be listed to the following standards as applicable:
(1)* ANSI/BHMA A156 Series for builders' hardware
(2) ANSI/UL 1034 for burglary-resistant electronic locking mechanisms
(3) ANSI/UL 437 for key locks
(4) ANSI/UL 768 for combination locks
(5) ANSI/UL 294 for access control system units
(6) UL Subject 2058 for high security electronic locks
(7) ANSI/UL 305 and ANSI/BHMA A156.3 for exit panic devices
13.7.3.3 Locking devices shall be properly installed and be in good working order.
13.7.3.4* Doors intended to be continuously secured shall automatically close and securely latch.
13.7.4* Key Control.
13.7.4.1 The integrity of key systems shall be protected by using key control.
13.7.4.2 Key control procedures shall include but not be limited to the following:
(1) Re-key when a key to a designated controlled or restricted area is lost
(2) Maintain access lists for persons authorized to draw master keys
(3)* Maintain security of key storage containers and cabinets
(4) Perform security checks of key storage containers and cabinets
(5) Inventory keys annually or as dictated by the security plan
(6) Maintain a written record of key issuance requests, approvals, and issuances
(7) Destroy or maintain security on keys not issued or no longer needed
(8) Discretely identify keys and key tags by using a coding system
(9)* Train employees on key control policy and procedure
13.7.4.3* Key control records shall include but not be limited to the following:
(1) Number assigned to each key and lock
(2) Location of each lock (room number)
(3) Person to whom keys have been issued
(4) Date of issuance
(5) Date of return
(6)* Documented acceptance for keys issued and returned
Substantiation: Proposed new text from NFPA 730, 2011 edition. NFPA 730 went through a complete revision in for the 2011 edition and that additional text for healthcare facilities is proposed for addition here.

99- Log #82 HEA-HES Final Action:
(13.11)

Submitter: Michael D. DeVore, State Farm Insurance
Recommendation: Revise to read:
13.8 Drills ~~11 Program Evaluation~~ .
13.~~11~~8.1* Periodic drills shall be conducted at various times and locations.
13.~~11~~8.2 The drills shall be critiqued for plan effectiveness and to identify opportunities for improvement.
13.~~11~~8.3 Identified opportunities for improvement shall be incorporated into the security plan.
13.~~11~~8.4 ~~The SVA and security plan shall be evaluated at least annually.~~
~~13.11.5~~ The evaluation of the security management plan shall include a review of laws, regulations, and standards applicable to the security program.
Substantiation: Renumber to match the reorganization of Chapter 13. Delete 13.11.4 because it is in direct conflict with 13.1.2.

99- Log #286 HEA-HES Final Action:
(A.12.1.1)

Submitter: Susan B. McLaughlin, MSL Healthcare Consulting, Inc.
Recommendation: Delete the second paragraph:
~~The Joint Commission has incorporated Comprehensive Emergency Management Plan, Annex G for The Joint Commission publications.~~
Substantiation: The sentence removed is unclear.

99- Log #287 HEA-HES Final Action:
(A.12.5.3.1.2)

Submitter: Susan B. McLaughlin, MSL Healthcare Consulting, Inc.
Recommendation: Revise text to read:
A.12.5.3.1.2 By basing the planning of health care emergency management on realistic conceptual events, the program reflects those issues or events that are predictable for the environment in which the organization operates. Thus, such conceptual planning should focus on issues, such as severe weather typical in the locale, situations that can occur due to close proximity of industrial, ~~government,~~ or transportation complexes, or earthquake possibilities due to local seismic activity. Planning should also incorporate knowledge available in the emergency management research about how individuals, small groups, organizations, communities, and societies behave during emergencies.
Substantiation: Proximity to government buildings is a significant vulnerability.

99- Log #288 HEA-HES Final Action:
(A.12.5.3.3.6.1(5))

Submitter: Susan B. McLaughlin, MSL Healthcare Consulting, Inc.
Recommendation: Revise the third paragraph to read:
It should be recognized that single-channel radio communication is less desirable than telephone system restoration due to the limited number of messages that can be managed. Cellular telephones, although useful in some disaster situations, should not be considered a contingency that has high reliability due to their vulnerability to the load control schemes of telephone companies. ~~Portable~~ Text messaging has been proven to be more reliable than cellular phone calls. Social media can be an important tool for emergency communication, but it must be managed so that responses to inquiries can be provided. Portable e-mail devices, satellite telephones, and audio- and video-conferencing services are useful tools to link key staff and organizations.
Substantiation: Additional information provided about current communication methods.

99- Log #65 HEA-HES Final Action:
(A.13.1)

Submitter: Michael D. DeVore, State Farm Insurance
Recommendation: Revise to read:
A.13.1 This chapter ~~is the source~~ provides those with responsibility ~~for securitymanagement in health care facilities and is based on the foundations of NFPA~~, the criteria to develop a security management plan. Additional information can be found in NFPA 730, Guide for Premises Security.
Substantiation: Explanatory material is from the body text. Then the duplicate material was deleted.

99- Log #69 HEA-HES Final Action:
(A.13.1.1)

Submitter: Michael D. DeVore, State Farm Insurance
Recommendation: Revise to read:
A.13.~~1~~2.1 A health care facility security plan can be formulated from security-sensitive areas that need the highest level of protection outward to the perimeter of the health care facility campus in concentric rings. Viewed from the outside, security is thus open and welcoming to patients and visitors. As an individual proceeds into the interior, public spaces might have minimal surveillance, but those sensitive areas that cannot be entered are layered with protections and countermeasures.
Substantiation: Renumber annex to match the reorganization in the body of the document.

99- Log #70 HEA-HES Final Action:
(A.13.1.2)

Submitter: Michael D. DeVore, State Farm Insurance
Recommendation: Revise to read:
A.13.~~1~~2.5 The security plan should be reviewed annually or more frequently if new challenges present themselves.
Substantiation: Renumbered to match changes to body text.

99- Log #71 HEA-HES Final Action:
(A.13.2.1)

Submitter: Michael D. DeVore, State Farm Insurance
Recommendation: Revise to read:
A.13.2.1 The security vulnerability assessment should be part of the HVA required by Chapter 4, Fundamentals. For general information regarding the SVA and premises security, see NFPA 730, Guide for Premises Security.
Substantiation: Renumbered to match revision of body text. Sentence added to explain the correlation between the HVA and the SVA.

99- Log #72 HEA-HES Final Action:
(A.13.2.4 (New))

Submitter: Michael D. DeVore, State Farm Insurance
Recommendation: Add a new section to read:
A.13.2.4 The risks identified in the SVA should be categorized by severity and frequency into building systems categories. The security plan should address risks according to the danger to patients and caregivers and then to the risk tolerance of the health care facility.
Substantiation: Added expanatory material on how to sort the SVA findings to organize them into categories that can be addressed for the safety of patients, caregivers, and other buidling occupants.

99- Log #289 HEA-HES Final Action:
(A.13.3.2(3)(c))

Submitter: Susan B. McLaughlin, MSL Healthcare Consulting, Inc.
Recommendation: Revise text to read:
A.13.3.2(3)(c) The emergency potential inherent in the telephoned bomb threat warrants inclusion of this contingency in the health care emergency operations plan. Experience has shown that facility personnel have to accompany police or military bomb demolition personnel in searching for the suspected bomb, because speed is of the essence, and only individuals familiar with a given area can rapidly spot unfamiliar or suspicious objects or conditions in the area. This is particularly true in health care facilities. The facility switchboard operator ~~has to~~ must be provided with a checklist, to be kept available at all times, in order to obtain as much information as possible from the caller concerning the location of the supposed bomb, time of detonation, and other essential data, which have to be considered in deciding whether or not to evacuate all or part of the facility.
Substantiation: Edit for language.

99- Log #67 HEA-HES Final Action:
(A.13.3.2(3)(c))

Submitter: Michael D. DeVore, State Farm Insurance
Recommendation: Revise to read:
A.13.3.2(3)(c) The emergency potential inherent in the telephoned bomb threat warrants inclusion of this contingency in the health care emergency operations plan. Experience has shown that facility personnel have to accompany police or military bomb demolition personnel in searching for the suspected bomb, because speed is of the essence, and only individuals familiar with a given area can rapidly spot unfamiliar or suspicious objects or conditions in the area. This is particularly true in health care facilities. The facility switchboard operator ~~has to be provided with~~ should have a checklist, to be kept available at all times, in order to obtain as much information as possible from the caller concerning the location of the supposed bomb, time of detonation, and other essential data, ~~which have to~~ which should be considered in deciding whether or not to evacuate all or part of the facility.
Substantiation: Revised text to non-mandatory language as required in the annex.

99- Log #74 HEA-HES Final Action:
(A.13.4, A.13.5, and A.13.6 (New))

Submitter: Michael D. DeVore, State Farm Insurance
Recommendation: Add new section to read:

A.13.4.1.1 Employee screening is typically a function managed by the human resources department.
The increase in the number of lawsuits based on the tort of negligent hiring has resulted in employers being under a greater responsibility to use due care in selecting employees. At the same time, federal and state laws impose restrictions on employers that are intended to protect the privacy of applicants. Since many employees have access to critical assets (people, property, and information), the need for pre-employment screening cannot be overemphasized.

A.13.4.1.1(1) Employers should conduct an appropriate level (based on the SVA and employee duties) of background screening varying from checking resources, criminal history, and credit, to a full background check with drivers' records, visual inspection of residence, interviews with known associates, and other formal checks. Polygraphs should be conducted only as permitted by law.

A.13.4.1.2 For large facilities, the use of color codes on identification badges should be considered and codes established for specific buildings, floors, or areas.

A.13.4.3 Patients who generate media interest should have special security procedures. VIP or media representatives bring a unique set of security requirements. Protection of VIPs is normally accomplished by restricting the use of names on charts and rooms and by assigning a dedicated security watch. Admission of a high-profile person to a health care facility creates two sets of problems that might require partial activation of the Health Care Emergency Management Plan: security and reception of news media. Provision of security forces in this situation might be provided by a governmental agency or private security forces. However, activation of facility security forces might be required to prevent curious onlookers from entering facility work areas and interfering with routine facility functioning. Routine visiting privileges and routine visiting hours might need to be suspended in parts of the facility.

A. 13.4.3.2.2 An escort can control movement of media personnel in the facility.

A.13.4.4 Crowd control of persons demanding access to care will create additional demands on security. Because of the intense public interest in disaster casualties, news media representatives should be given as much consideration as the situation will permit. Ideally, news media personnel should be provided with a reception area, with access to telephone communication and, if possible, an expediter who, though not permitted to act as spokesman for news releases, could provide other assistance to the news media. The marketing department of the hospital might be best suited to assist security personnel with media control. News media personnel should not be allowed into the health care facility without proper identification. To alert off-duty health care staff and to reassure the public, use of broadcast media should be planned. Media representatives should be requested to wear some means of identification for security purposes. Where feasible, photo identifications or other means to ensure positive identification should be used. Visitor and crowd control creates the problem of distinguishing staff from visitors. Such identification should be issued to all facility personnel, including volunteer personnel who might be utilized in disaster functions. Note that care should be taken to ensure that identification badges are recalled whenever personnel terminate association with the health care facility. Members of the news media should be asked to wear some means of identification, such as press cards, on their outside garments so that they are readily identifiable by security guards controlling access to the facility or certain areas therein. Clergy also frequently accompany casualties or arrive later for visitations and require some means of identification.

A.13.4.5 Security personnel can be an effective and useful component of a facility's physical security program.
The effectiveness of alarm devices, physical barriers, and intrusion detectors can depend on a response by security personnel.
Security services can be used for, but are not limited to, the following circumstances:
(1) The mission of the facility is particularly critical.
(2) There is a high level of sensitivity of information handled at the facility, such as national security information.
(3) An in-house response capability is needed, for example, the facility contains alarmed vaults or other sensitive operations, and off-site security personnel or police are not close enough for quick response.
(4) The facility is vulnerable to theft or damage, for example, a facility location in a high-crime area.

(5) Pedestrian or automobile traffic is heavy or congested and requires special controls.
(6) Valuable goods are stored or used in the facility.

As with any expenditure of funds for security, the annual costs of security services normally should not exceed the monetary value of the protected items.
A substantial expense for security services can be required for crowd or traffic control, for safeguarding highly classified or sensitive information, or for protecting material or functions that have high intrinsic rather than monetary value. This is especially true as applied to the safety of employees, since it is impossible to put a dollar value on human lives or peace of mind. A security post in a high-crime area can yield substantial benefits in terms of improved safety, higher employee morale, and increased productivity.

A.13.4.5.1.2(5) The disclosure should be in compliance with legal, regulatory, and contractual requirements.

A.13.4.5.2 Security personnel can perform the following services:
(1) Entrance control. Operate and enforce a system of access control, including inspection of identification credentials and packages.
(2) Roving patrol. Patrol routes or designated areas, such as perimeters, buildings, vaults, and public areas.
(3) Traffic control. Direct traffic (vehicular and pedestrian), control parking, check permits, and issue citations.
(4) Key control. Receive, issue, and account for certain keys to the building and its internal areas.
(5) Security and fire systems. Monitor, operate, and respond to intrusion and fire alarm systems or protective devices.
(6) Utility systems. Monitor, record data, or perform minor operations for building utility systems.
(7) Lost and found. Receive, provide receipts for, and store found items.
(8) Reports and records. Prepare reports on accidents, fires, thefts, and other building incidents.
(9) Response to emergencies. In case of any emergency (e.g., fire, bomb threat, assault, or civil disturbance), respond, summon assistance, administer first aid, and assist public safety personnel.
(10) Law and order. Maintain law and order within the area of assignment.
(11) Hazardous conditions. Report potentially hazardous conditions and items in need of repair.

A.13.4.5.2.2.3 Security personnel should be covered by liability insurance. Check for adequate liability insurance when contracting security services.

A.13.4.5.3 These methods are most effective when applied in conjunction with a system that ensures the patrols are actually performed. Such systems include watchclock service, electronic guard tour monitoring, and watchman systems. These systems provide a documentary record of the locations in the facility that were visited and the times at which each location was visited. Regular review of these records can help to ensure that security personnel are performing their patrols as planned.

A.13.4.5.3.1 Some ways to accomplish supervision are spot checks, daily logs, watch clock tours, and activity reports.

A.13.4.5.3.2(4) Signs of vandalism as well as signs of transients or vagrants living on or around the property should be noted. Security-related complaints made by employees or tenants should be noted as well.

A.13.4.5.5 Security personnel should be armed only when there are compelling reasons. If security personnel are armed for a deterrent effect, that is, to prevent crime or other unauthorized activity, responsible officials must weigh that advantage against such disadvantages as the danger to innocent personnel if a firearm is used by a security person; the possibility of an accidental discharge; and the possibility, no matter how remote, of irrational behavior on the part of security personnel. Many states have laws that require background checks and specific training for security personnel, especially armed personnel.

A.13.4.5.6 It is essential that facilities using security personnel train them in the legal and practical applications of their employment. Training should be repeated periodically. Training must reflect changes in regulations and the enactment of new laws.

A.13.5.1.1 While shipments typically arrive by truck, shipments also can come in through other transportation modes such as trains or barges.

A.13.5.2.2 See A.6.3.3.1 for characteristics indicating a suspicious package.

A.13.5.3.1 Suspicious packages or mail should not be opened. Suspicious mail may show any or all of the following characteristics:
(1) No return address
(2) Mailed from a foreign country
(3) Excessive postage
(4) Restrictive markings like “Personal” or “Special Delivery”
(5) Misspelled information in the address
(6) Addressed to a title rather than an individual
(7) Badly typed or written
(8) Powdery substance felt through or appearing on the package or envelope
(9) Lopsided or uneven in shape
(10) Rigid or bulky packaging
(11) Strange odor
(12) Oily stains, discoloration, or crystallization on the packaging
(13) Excessive packaging material such as masking tape or string
(14) Excessive weight
(15) Ticking sound
(16) Protruding wires or aluminum foil
Consideration should be given to receiving mail in an area separated from critical functions.

A.13.6.1.2 The primary security perimeter might contain areas that are not contiguous. The noncontiguous U.S. states, Hawaii and Alaska, are well-known examples.

A.13.6.1.3 The primary security perimeter can include multiple secondary security perimeters. It is possible for a secondary perimeter to be congruent with the primary perimeter.

A.13.6.1.4 Secured perimeters are physical barriers that control authorized access to secure areas. Physical barriers can be of two general types: natural and structural. Natural barriers include mountains, cliffs, canyons, rivers, or other terrain that is difficult to traverse. Structural barriers are man-made devices, such as fences, walls, floors, and roofs.

A.13.6.2 There are few security plans where access is intended to every area. Accordingly, access to some areas is necessarily secured.
The following areas should be designated as controlled areas:
(1) An area where confidential information or highly sensitive information is handled, processed, or stored (e.g., a mailroom)
(2) An area that houses equipment that is significantly valuable or critical to the continued operations or provision of service
(3) An area where uncontrolled access would interfere with or disrupt personnel assigned to the area in carrying out their official duties
(4) An area where equipment or operations constitute a potential safety hazard
(5) An area that is particularly sensitive as determined by the responsible manager
The following areas should be designated as restricted areas:
(1) An area that houses mainframe computers or designated sensitive information systems
(2) An area that is highly critical or sensitive as determined by the responsible manager
Substantiation: These are the Annex sections to go with the new text from NFPA 730, Guide to Premises Security, 2011 edition.

99- Log #76 HEA-HES Final Action:
(A.13.4.2(1), A.13.4.3(5), A.13.4.4, A.13.4.6(3),)

Submitter: Michael D. DeVore, State Farm Insurance
Recommendation: Revise A.13.4.2(1) , A.13.4.3(5) , A.13.4.4 , A.13.4.6(3) , A.13.4.7(1) as follows:
A.13.46.3.2(1) A visible presence is normally accomplished by the placement of a security officer at the ambulance entrance. This serves the dual purpose of monitoring the security cameras throughout the emergency department as well as the activity at the ambulance entrance.
A.13.46.3.3(5) The facility-wide alerting system should be activated for all reports of pediatric or infant abduction. The use of a standardized “code alert” system can facilitate the announcement; for example, “code pink” for an infant abduction or “code purple” for a pediatric abduction.
A.13.46.3.4 Video surveillance and motion detection can be used as additional protection for these areas. Some controlled drugs might need to be stored in safes.
A.13.46.3.6(3) Reasons for a contraband check procedure would be to control items such as tobacco, drugs, or tools that could cause harm to the patient or staff.
A.13.46.3.7(1) Law enforcement personnel should have orientation on the emergency procedures and layout of the facility. There should be good communication between law enforcement and health care facility security staff.
Substantiation: Revise numbering to match public input #75.

99- Log #290 HEA-HES Final Action:
(A.13.4.4)

Submitter: Susan B. McLaughlin, MSL Healthcare Consulting, Inc.
Recommendation: Revise text to read:
A.13.4.4 Video surveillance and motion detection can be used as additional protection for these areas. Some controlled drugs ~~might need to~~ should be stored in safes.
Substantiation: Edit language.

99- Log #80 HEA-HES Final Action:
(A.13.5.3.1)

Submitter: Michael D. DeVore, State Farm Insurance
Recommendation: Revise to read:
A.13.~~5.3.1~~ 6.4 There can be times where full or partial facility access or egress is not desirable. Planning for these events should be conducted in coordination with local emergency agencies, such as police, fire, and public health agencies.
Substantiation: Numbering revised to match public input for the body text.

99- Log #83 HEA-HES Final Action:
(A.13.6, A.13.6.1.1, A.13.6.2, A.13.7, A.13.8.3, A.13.9, A.13.10, and A.13.10.1)

Submitter: Michael D. DeVore, State Farm Insurance
Recommendation: Delete all of A.13.6, A.13.6.1.1, A.13.6.2, A.13.7, A.13.8.3, A.13.9, A.13.10, and A.13.10.1.
Substantiation: The body text was deleted by a previous public input and the proposed complete revision of Chapter 13. The annex text is moved to people management and portal control sections.

99- Log #79 HEA-HES Final Action:
(A.13.7 (New))

Submitter: Michael D. DeVore, State Farm Insurance
Recommendation: Add new sections to read:
A.13.7.1.2 Access through portals is usually controlled for ingress, but it is possible to control movement in both directions. The decision to control in both directions is based on the SVA. When portals are not staffed, they should be locked, illuminated during the hours of darkness, and periodically inspected. Semi-active entrances, such as railroad siding gates or gates used only during peak traffic flow periods, should be locked except when actually in use.

A.13.7.3.1 More information on fire resistance–rated opening protectives is in NFPA 80, Standard for Fire Doors and Other Opening Protectives.

A.13.7.3.2(1) ANSI/BHMA A156 performance guides include security tests .

A.13.7.3.4 Doors that are always locked should have a latch-type lock and closer to ensure they are not accidentally left unlocked.

A.13.7.4 The integrity of a key system is important to safeguarding property and controlling access. Lost or stolen keys and key blanks can compromise the security of a key system. The security officer should ensure that responsible individuals maintain control over the facility's key system by storing, issuing, and accounting for all keys under the facility's control. Issuance of keys should be kept to a minimum. Keys should be issued only to persons who have an official need.

PC-based software, key storage cabinets, and computer-controlled key retention and distribution systems are available to facilitate the management of a master key system and help to ensure its long-term integrity.

Facility keys should not be identified in any manner such that a person finding a lost key could trace it back to the facility. A policy should be established to restrict duplication of keys without written permission. All keys should be marked “DO NOT DUPLICATE” to deter the unauthorized copying of keys.

A master key system should be designed so that the grandmaster key is the only key that will open every restricted area of the facility. A master key system is used to limit the number of keys carried by personnel requiring access to multiple areas of the building. It is important that such a system not be designed so that the loss of a single key could provide an unauthorized person unrestricted access to all areas of the building. The sophistication of the master key system should depend upon an assessment of employees’ or tenants’ needs and the criticality, risk, and sensitivity of restricted areas. The number of grandmaster keys should be limited to the least number necessary for operation of the facility. Master key distribution should be limited to the personnel requiring access to multiple restricted areas.

A.13.7.4.2(3) Key storage containers and cabinets should be kept locked with a pick- and drill-resistant, patented high security cylinder that is not keyed to the facility master key system.

A.13.7.4.2(9) Key control policies should do the following:

(1)Remind employees to keep official keys on their person or securely locked in a desk or cabinet.
(2)Have a policy against lending keys to an unauthorized person.
(3)Require employees to promptly return official keys checked out on a temporary basis.
(4)Require reporting of lost or stolen keys immediately to the appropriate official.
(5)Establish procedures for collecting keys from terminated employees, employees on vacation, and vacated tenants.

A.13.7.4.3 Records of key issuance should be secured and kept separate from keys.

A.13.7..4.3(6) There are many ways to document the acceptance for keys. The recipient can sign the key control record, use a machine readable credential, or be tracked with an electronic key control system.
Substantiation: Annex for new materail submitted for Section 13.7. Text from NFPA 730, 2011 edition.

99- Log #291 HEA-HES Final Action:
(A.13.8.3)

Submitter: Susan B. McLaughlin, MSL Healthcare Consulting, Inc.
Recommendation: Add a new first paragraph to read:
A.13.8.3 Key cards are preferable to traditional keys because they can be immediately deactivated if lost or not returned by a terminated employee.
Substantiation: This input updates the material to include current technology commonly in use that would eliminate many of the concerns that are subsequently identified in this section.

99- Log #84 HEA-HES Final Action:
(A.13.11.1)

Submitter: Michael D. DeVore, State Farm Insurance
Recommendation: Revise to read:
A.13.~~11~~8.1 ~~The effectiveness of the security plan is tested by performing drills.~~ Drills should be conducted on all work schedules~~. Drills during all shifts are necessary~~ so that all personnel are familiar with the plan. Practicing the plan helps personnel react as needed during a security incident.
Substantiation: Revised the numbering to match the body text revision. Also deleted the first sentence as unneeded. Deleted the part about being necessary as this indicates the drill is mandatory, which is not permitted in the annex material.

99- Log #292 HEA-HES Final Action:
(B.12.1.1.4)

Submitter: Susan B. McLaughlin, MSL Healthcare Consulting, Inc.
Recommendation: Add a new last paragraph to read:
Hard copies of the EOP need not be widely distributed. Staff members need access to incident-specific plans, but not the entire dorcument. Several copies of the full EOP should be available in the Hospital Command Center, the administrative offices, and with the chair of the Emergency Management Committee. Posting the EOP on the hospital intranet with linkages to enhance movement through the plan can also be very effective, however a few hard copies should still be available in the event of computer failure.
Substantiation: The current version of this section addresses distribution but does not identify to whom the plan should be distributed. This input limits the distribution of the EOP.

99- Log #293 HEA-HES Final Action:
(B.12.3.2.8(1))

Submitter: Susan B. McLaughlin, MSL Healthcare Consulting, Inc.
Recommendation: Revise text to read:
(1) Transportation, including knowledge of which roads are open and actually transporting staff to the facility. Any transportation provided to staff should be by hospital drivers in hospital vehicles to avoid liability.
Substantiation: Many hospital EOPs include volunteer staff members picking up other staff members in their personal vehicles. This is not advisable due to the hospital's liability in the event of an accident.

99- Log #294 HEA-HES Final Action:
(B.12.3.3(1))

Submitter: Susan B. McLaughlin, MSL Healthcare Consulting, Inc.
Recommendation: Revise text to read:
(1) Move to predesignated areas, whether in the facility, nearby, or in remote zones. Evacuation directives will normally indicate destinations. Note that it is recommended to predesign a mutual aid evacuation plan with other health care facilities in the community. (See Annex D, U.S. Government Publication 3152, Hospitals and Community Emergency Response — What you Need to Know, on the subject of health care community mutual aid and evacuation planning.) In some communities, receiving hospitals are designated by EMS services based on availability.
Substantiation: This input recognizes that pre-determined mutual aid agreement may not be necessary in communities where EMS manages the evacuation.