
# Break-Glass – An Approach to Granting Emergency Access to Healthcare Systems

This Paper was developed by the
Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC)

This Paper has been approved by:
NEMA (National Electrical Manufacturers Association-USA)
COCIR (European Coordination Committee of the Radiological and Electromedical Industry)
JIRA (Japan Industries Association of Radiological Systems)

December 2004



Secretariat: NEMA (National Electrical Manufacturers Association) www.nema.org/medical
1300 North 17th Street, Suite 1847, Rosslyn, VA 22209 USA tel: 703-841-3200 fax: 703-841-5900
Secretary: Stephen Vastagh, tel: 703-841-3281; fax: 703-841-3381 E-mail ste_vastagh@nema.org

# 1. Purpose and Scope

This white paper discusses a simple yet effective emergency-access solution, sometimes called "break-glass". The purpose of break-glass is to allow operators emergency access to the system in cases where the normal authentication cannot be successfully completed or is not working properly. The systems include medical data acquisition devices as well as information systems which are collectively referred to as Medical Information Systems (MedIS[1]).

Break-glass is based upon pre-staged "emergency" user accounts, managed in a way that can make them available with reasonable administrative overhead. This solution can be used with a broad range of existing systems and architectures that require operators to login, such as with username and password, before access is granted.

The break-glass solution is time-tested, robust, and does not require additional automated technology. It is intended to specifically cover emergency cases and should not be used as a replacement for a helpdesk.

This white paper is aimed at MedIS and healthcare IT management personnel. The SPC suggests that they develop an emergency access system, taking into account the emergency access capabilities described in this paper.

# 2. Introduction

Historically, many MedIS could be used without identifying and authenticating the user. However, regulations around the world, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States[2], and EU Directive 95/46/EC[3] in the Member States of the European Union, have made it clear that individually-identifiable medical data needs to be protected while making that data available to authorized individuals.

A user authentication system is one of the typical mechanisms used to control and monitor access to sensitive data. Many such systems employed in MedIS today are based on authentication architectures of general-purpose information systems. They are designed to preserve security by

[1] MedIS generally includes all information systems directly employed in delivering health care. Examples include, but are not limited to: HIS (Hospital Information System), PACS (Picture Archiving and Communication Systems), imaging modalities, radiation therapy systems, cardiology information systems, and patient monitoring systems.

[2] HIPAA states covered entities need to restrict access to all forms of protected health information:

- §164.312(a)(2)(i) *Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity.
- §164.312(d) *Standard: Person or entity authentication.* Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

[3] EU Directive 95/46/EC states:

- Article 17 (1) … the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. …

restricting access, above all else, and "fail-closed." Fail-closed systems work well in some industries and settings (e.g., financial, insurance, manufacturing, national security) since a delay in access by an authorized user to the functions performed by the system or to the data contained within will generally only cause inconvenience.

In healthcare, a delay in access to a MedIS is likely to disrupt patient care which may cause patient discomfort, additional injury or worse. For this reason HIPAA requires covered entities to have contingency plans in place that assure patient care is not impaired by problems with the user identification and authentication system of the MedIS.

# 3. Contingency Planning

Sites currently recognize the need to conduct a risk assessment and prepare for unusual events such as power outages, fire, and flood. Preparation includes developing fallback plans and practicing them ahead of time so that everyone understands what to do when the situation arises. Similar preparation is required for instances where normal user identification and authentication is not possible and might endanger proper delivery of healthcare. The need for such emergency planning is required by the HIPAA Security Rule[4]; and it is implied by the harmonized European legislation.

An emergency access solution should be used only when normal processes are insufficient, e.g. the helpdesk is unavailable. Some cases where emergency access might be necessary include:

A. account problems:
- Forgotten Username/Password, e.g. after prolonged absence (illness, vacation)
- Locked Password, e.g. mis-typed too many times
- No User Account, e.g. a medically competent individual is assisting a facility during an emergency, or

B. authentication system problems:
- Enterprise Authentication System Failure, e.g. a centralized authentication server is down
- Smart Card Reader Failure, e.g. card or reader damaged
- Biometric Mechanism Failure, e.g. reader is malfunctioning or biometric is damaged

C. authorization problems:
A. An emergency medical situation thrusts an operator into a role where she lacks sufficient access rights, e.g. clerk is entering orders during an emergency.

[4] HIPAA states: "Covered Entities need to anticipate emergencies and develop plans-of-action to deal with them"
- §164.308(a)(7)(ii)(C) *Emergency mode operation plan* (required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
- §164.312(a)(2)(ii) *Emergency access procedure* (required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

In cases where the authentication system fails, there should be an alternate authentication mechanism such as username/password.

# 4. The Break-Glass Solution

The break-glass solution is based on pre-staged emergency user accounts, managed and distributed in a way that can make them quickly available without unreasonable administrative delay. This solution follows the guideline that contingency plans should be simple, effective, and reliable.

## *4.1. Pre-staging Accounts*

Emergency Accounts should be created in advance to allow careful thought to go into the access controls and audit trails associated with them. When creating the prestaged emergency accounts, the site administrative privacy and security policy must be consulted. The following factors should be considered:

A. Username should be obvious and meaningful, e.g. *emergency001* so the account will be obviously inappropriate for normal operations and will stand out in audit trails.
B. Passwords should be hard to guess or crack, within the limitations of the MedIS. It is important, they not be so difficult that the user, in an emergency, would have trouble entering it.
C. Account Permissions should be set to ***least necessary privilege*** based on the results of a risk assessment, e.g. grant access by emergency users to the minimum data and functionality needed to perform their task. This could potentially include view-only capability, prohibiting access from outside the local console or network, limiting to data acquisition only, or prohibiting access to previously acquired data. Due to the difficulty of anticipating emergency needs, sites may choose to allow full access to emergency accounts.
D. Auditing should be enabled if available to log details of the account usage and details of the work carried out while using the account. Some systems may recognize emergency accounts and raise the system auditing level or increase audit logging of only the emergency accounts.

Care needs to be taken to ensure that the people who create the accounts are not the ones reviewing the audit trails since those who know account details can be a source of abuse. In addition, the accounts and distribution procedures should be tested to assure quick access when they are needed.

## *4.2. Distributing Accounts*

Prestaged accounts need to be carefully managed to provide timely access when needed. Break-glass requires that the emergency-account details be made available in an appropriate and

reasonable manner. These details may be provided on media such as a printed page, a magnetic-stripe card, a smart card or a token. Some distribution possibilities for break-glass emergency accounts include the following:

A. Kept behind glass in a cabinet, where access to the accounts requires literally breaking the glass (similar to a fire extinguisher or alarm), providing an obvious indication that the accounts have been accessed and a deterrent to casual use;
B. Maintained within sealed envelopes, where a broken seal would be an obvious indication that the accounts have been accessed;
C. Locked in a desk drawer that only specific people can access, e.g., Charge Nurse or a facility security guard;
D. Sealed and taped to the side of a monitor at the nurse station – visible to many so it will be obvious when it is missing or damaged, or
E. For cases where more than one person is needed to declare an emergency, locked in a safe or cabinet where one person knows the combination or has the cabinet key and a different person has the key to the room.

A best-practice would place the pre-staged emergency accounts into the responsible care of an individual. This Emergency Account Manager would be someone readily available during operating hours and one who understands the sensitivity and priority of the emergency accounts (e.g. a shift-manager, charge nurse or security officer). The distribution procedure would include a sign-out method requiring that an acceptable form of identification be provided. This identity would be recorded before the accounts are made available. Following such a procedure assures that activities performed using the emergency account may eventually be associated with an authorized individual, creates accountability and can assure non-repudiation.

## *4.3. Monitoring Use of Accounts*

The use of emergency accounts needs to be carefully monitored. The audit mechanisms within the MedIS should be used and a procedure defined to examine the security audit trails on a regular basis to identify any use of the emergency accounts. In addition, systems can alert the security administrator in the event an emergency account is activated. These enhanced capabilities are highly desirable, but thay are not required for the break-glass mechanism to work.

If the MedIS cannot provide an audit trail that shows simple account activity like login attempts, then the use of break-glass needs to be carefully considered before implementing. Break-glass may still remain a valid system, but it will require the use of a manual (e.g. paper-ink) log.

Site policy should describe the intended use of such accounts and the consequences of their inappropriate use. Details should be clearly documented and then communicated to the relevant workforce. It should be clear that all use of emergency accounts is closely monitored. A periodic review and retraining of staff should be done to make sure the break-glass procedure continues to be relevant.

Each use of an emergency account should be reviewed. The use of an emergency account may be valid, or it might indicate a malicious act. Unacceptable use needs to be recorded and acted upon. Frequent use may indicate problems with the normal user authentication mechanism.

This regular monitoring of pre-staged emergency accounts should also include exercising some of them to ensure that they do work, and that their use can be detected. This is similar to testing fire alarms, to be sure that they will work in a real emergency.

### *4.4. Cleaning Up After Account Usage*

A procedure should be established to clean up after an emergency account has been used. Consider addressing the following:

A. Disable or delete the emergency account(s) that were used to prevent re-use now that the password is known. The MedIS may be capable of automatically deactivating emergency accounts after first use or passage of a selectable period such as 8 hours or 1 day. Avoid disabling the account during the period of emergency use.
B. Reconcile the data acquired and audit trails to reflect the proper operator's name.
C. Make entries in "disclosure logs" if appropriate.
D. Review activities performed including data acquired/accessed according to the site policy.
E. Determine if the emergency account procedure and operation worked effectively and adjust if necessary.
F. Create and distribute new accounts for future break-glass use. Assigning new passwords to a used emergency account may not be appropriate under the local security policy.

Monitoring and cleanup of accounts may be complicated if the same account is available from multiple distribution points. This can be avoided by making the details of each account available at only one location.

## 5. Conclusion

There are many good reasons to implement a solution for emergency access to patient data. Patient care is paramount. The HIPAA Security Rule, the corresponding European legislation, and privacy rules in Japan all promote emergency access solutions. The break-glass solution described in this white paper is easy to implement with existing medical systems, can be adapted to virtually any user authentication system, protects patient privacy, and can provide acceptable user accountability, all while ensuring continuous availability of healthcare for patients. For new system designs, automated solutions may be available, but break-glass is a proven, robust mechanism that is reasonable, appropriate, and cost effective for existing systems in any healthcare enterprise.