* Recent FHIR (4/19/17 post) on “Break The Glass” -- **Example Instance**

®© HL7.org 2011+. FHIR Release 3 (STU; v3.0.1-11917) generated on Wed, Apr 19, 2017 07:49+1000.

<http://www.hl7.org/FHIR/operationoutcome-example-break-the-glass.ttl.html>

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

* **Guide to the HL7 Health Care Privacy and Security Classification System**

Guide to the HL7 Health Care Privacy and Security Classification System Page 25 September 2013 © 2013 Health Level Seven International. All rights reserved.

**[See the yellow highlighted section below. The entire official HL7 Guide is also attached to this email. This is only an excerpt from the Appendix A. Tom Sullivan, MD]**

***APPENDIX A: TABLE OF DEFINITIONS 555***

|  |  |
| --- | --- |
| **Table A: Table of Definitions 556 Term**  *Note that hyperlinked terms are either links back to text or to related terms.* | **Definitions and Descriptions**  *Note that where no source is specified, the terms are defined in the context of HCS. Some entries are authoritative descriptions about the use of the term and may contain the term being defined in this glossary. These descriptions are not considered definitions.* |
| Access Control Service | A service that provides the basic operational aspects of access control such as making access control decision information (ADI) available to access decision components and performing access control functions. The service also provides security labeling and privacy and security protection functions.  The service, known as an Access Control Service (ACS), requires the following information:  Access policy rules,  Contextual information needed to interpret ADI,  Initiator, target, and access request ADI,  Security labeling rules and vocabulary,  Transform rules and services.  ACS generates information made available to other elements includes transformed information response to an information request as well as handling caveats. |
| Access (Security) Level | The combination of a hierarchical security classification and a security category that represents the sensitivity of an object or the security clearance of an individual. [ISO 2382-8/T-REC-X.812-199511-I!!PDF-E]  A level associated with an individual who may be accessing information (for example, a clearance level) or with the information which may be accessed (for example, a classification level).[ HIPAA Security Glossary] |
| Break the Glass | “Break the glass” access barriers are application generated warnings at the moment of possible transgression that requires users to assert their need for access. Distinguish break glass from emergency access. In the case of break glass no additional user permissions are required (similar to a fire alarm in a hallway, all users have access to the alarm); however, access may involve alerts to system managers and increased auditing. Examples of break glass include access to one’s own records, to records belonging to a spouse, family member or to a VIP. In contrast to emergency access, break glass does not require evaluation of patient consent directives, nor is eminent threat to patient safety a concern.    Security Work Group Emergency Access paper |
| Classification  *Child concept:*  *Security Classification* | Confidential protection of data elements by segmentation into restricted and specifically controlled categories set by policies, professional practice, and laws, legislation, and regulations. [Adapted from ASTM E-1986] |
| Clearance | Initiator-bound access control information (ACI) that can be compared with security labels of targets. [ISO 10181-3/ITU X.812] |
| Permission granted to an individual to access data or information at or below a particular security level. [ISO/IEC 2382-8:1998] | |
| Clinical attribute | Any clinical characteristic that binds a health care relevant parameter to a clinical element by a rule. Parameters may include authorship, category of information, terminological characteristics, history of permutations, integrity and provenance, as well as the relationship to and inclusive of associated clinical facts necessary to provide context essential for applying security labels. [PCAST discusses attributes that provide context to clinical data elements such as patient demographics.] |

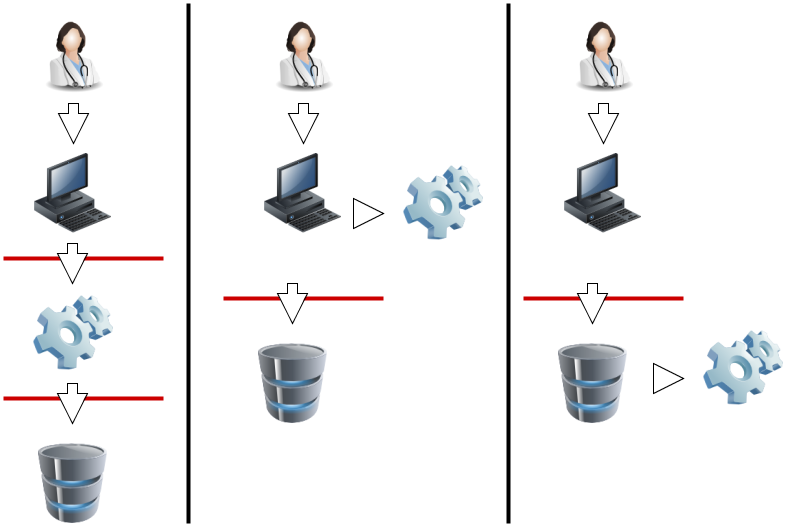
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

**Optional Blog mentioning OAuth scopes from December 2015**

**Sunday, December 27, 2015**

### **Break-Glass on FHIR solution by** [John Moehrke](https://apis.google.com/u/0/wm/1/111566682979991899107)

I explain the use-case and environment behind [Break-Glass on FHIR.](http://healthcaresecprivacy.blogspot.com/2015/12/break-glass-on-fhir.html) In there I explain that it is unusual to need Break-Glass, but that it is still an important capability in healthcare.  In this article I will outline a few solutions that exist, and hint at some other solutions.  
  
This solution is based on a Client/Server relationship where the security subsystem is managing Access Control between the Client and the Server. This diagram and definitions from the FHIR [specification](http://hl7.org/implement/standards/fhir/security.html)

[](http://hl7.org/implement/standards/fhir/security-layout.png)

 Where:

|  |  |
| --- | --- |
| https://lh4.googleusercontent.com/proxy/8VW4ay581ZymnJagi7byRAnDCGTcetJQ09GPUR0Gttxu-xmoGM6Aq0kmK9GtHcFODJWogmahO_Lx02X9CphFCxblPzTPFlH3L6lWfZc2cZhBFw=s0-d | The consumer that is using a healthcare related system |
| https://lh5.googleusercontent.com/proxy/fldtJ_7_a8404x2xK_FW4Z5sC_6LFmfSG6Rp95Efd74MLAnONK4H4x99sR73LKQ7Ejk9ESCT--AnMNd-kklUrc0ywJ-kf9LZYZsGa7JlxRA2=s0-d | The client application the user is using (application, mobile app, website, etc.) |
| https://lh6.googleusercontent.com/proxy/aGhk7WPOTNh8rh4Nq1xw8TsnPWqFfv0ePK203jLakBY3nnmJWBpQiH9EnIuBpdVJjuBSZgzHi3t69KIgHMpc6NOFv81vgV99rtjyR-c40LZi=s0-d | The security system (authentication and access control) |
| https://lh3.googleusercontent.com/proxy/Y3LDo5AMYrleF8Bedw5772WMv2s8BKhBPnCPFADb4uYpqXUbu0zgFLDoDehu2sKUZMsJFy2r2YrcqdqMU0xl23jOpMqJD9A8RoRDaHA_34gK4A=s0-d | The clinical/healthcare repository |

**Notify that Break-Glass 'could' be used.**

This is not specifically necessary, as a user/system could always indicate that Break-Glass is being invoked. If it is not authorized, then this request would be rejected. If it is authorized by no new information then nothing more is returned. The problem is that without a way to notify that break-glass could be used, then the degenerate system results: Either normal RBAC, or it is always an emergency. Thus for true Break-Glass, one really needs a way to indicate that information is being withheld that could be accessed if Break-Glass was declared. Note that this notification should not be used when there is data being withheld that is not accessible under Break-Glass.  
  
The way that is in the FHIR Specification today is to include in the [OperationOutcome.issue.code](https://www.hl7.org/fhir/operationoutcome.html#def) the value "[suppressed](https://www.hl7.org/fhir/valueset-issue-type.html)", with severity at "[informational](https://www.hl7.org/fhir/valueset-issue-severity.html)".  This would indicate that for a normal request that the normal results were returned (Informational but suppressed). This does require that suppressed is not used for any other purpose. This is not obvious today, but could be an operational requirement in a specific environment, likely under some Implementation Guide.  
  
As discussion on the FHIR mailing list have shown, not all operations can easily have both success and also have an OperationOutcome resource, so this model only works where OperationOutcome can be carried on the Response.

**Indicate that Break-Glass is being used.**

On the [Security-Labels](http://hl7.org/implement/standards/fhir/security-labels.html) page is a [proposal for how to indicate that Break-Glass is requested](http://hl7.org/implement/standards/fhir/security-labels.html#break-the-glass). I don't recall reviewing this text, so it was a surprise when Grahame pointed it out to me. It seems odd to be on the Security-Labels page rather than the [Security](http://hl7.org/implement/standards/fhir/security.html) page. It doesn't even use a security label.  
  
This solution proposes that a URI could be defined to indicate that "Break-Glass" is being requested. This URI is then represented in the HTTP Request as a [web category.](https://tools.ietf.org/html/draft-johnston-http-category-header-02)  
  
I would see this as more experimental, but given that it is in the specification today, I must at least acknowledge that it is more than just something for people to experiment with and give us comments. That said, if you have comments, I would be very happy to receive them.

**Audit Log that Break-Glass has been used.**

When Break-Glass is used it is important to record in the audit log that Break-Glass was used. This triggers the Privacy and Security office working with the Clinical Safety office to investigate if it was appropriate use of Break-Glass. In FHIR [AuditEvent,](http://hl7.org/implement/standards/fhir/auditevent.html) there is a defined way to indicate that Break-Glass has been used. Benefit of basing this on [ATNA](http://healthcaresecprivacy.blogspot.com/2013/01/simplifying-security-audit-standards.html). Here is the critical aspects:

AuditEvent.type --> 110113, Security Alert   
AuditEvent.subtype --> 110127, Emergency Override Started   
AuditEvent.recorded --> When it happened  
AuditEvent.agent --> Who declared break-glass  
AuditEvent.agent.location --> Where is this agent  
AuditEvent.agent.policy --> Policy enabling break-glass  
AuditEvent.outcomeDesc --> Free-text explanation of  why  
AuditEvent.purposeOfEvent --> Why break-glass(ETREAT)

Where an entry in AuditEvent.outcomeDesc, could carry the 'text' description that the user is prompted to enter. This is a common UX for Break-Glass, where the user must type in a free-text explanation of why they feel it is warranted to 'break-glass'.

Followed later, hopefully, by 110138, Emergency Override Stopped. This is not always possible to know, as not all user experiences are specifically session oriented. But often times the user experience is clear when the event starts and when it stops.

**Future experimentation on Break-Glass**

This is a good experimentation topic. I don't think the best solution has yet been found. So here are a few alternatives to play with.

**Using Security-Labels**

The security-labels include the full vocabulary from the Healthcare Privacy and Security Classification System (HCS), so there are security tags that can be used to indicate for each Resource instance if it is "Normal" or "Restricted". Thus the data that falls into the "Break-Glass" use, would be marked "Restricted", while "Normal" (or less) would be available for "Treatment".

This is the most likely way to identify information that should be blocked except for "Break-Glass", but is not specifically necessary. This solution does require well managed tags on all data.

**Using OAuth for Break-Glass**

One thought I have is to leverage OAuth 'scope'. In normal operation one would always ask for an OAuth token using a scope value that limits access to "Treatment", which would be 'normal treatment'. When needing to declare Break-Glass, one would ask for a OAuth 'scope' with "Emergency Treatment". In this way, the OAuth authority can reject, because the user doesn't own the rights to Break-Glass, or if it does return the security-token it is an indication to the Server that Break-Glass has been declared and given to the user.

**Using side-channel requests**

A classic solution is to provide an alternative service that one could query to see if information would be suppressed. You would send the request you would like to ask a Server, and you get back an indication of if information would be suppressed without Break-Glass. The problem this has is that it requires another round-trip.

**Conclusion:** Not done yet... need experimentation and lessons-learned sharing... so please share.