HIPAA Security Policies for the dash.catalyzecare.org Server

164.308 Administrative Safeguards

a 1 Security Management Process

A Risk Analysis

HUBzero will take reasonable steps to identify and prioritize the risks to the confidentiality, integrity, and availability of EPHI due to applications that access the EPHI only by means of SSH tunnel, excluding those applications that access EPHI by other means. For this purpose, a risk analysis will comprise:

- An inventory of which directories contain EPHI, who should have access to these directories, and any special policies required of these directories by any associated business associate agreement.
- An identification of potential threats to the confidentiality, integrity, and availability of EPHI.
- An identification of weaknesses that may facilitate the realization of threats.
- An assessment of existing controls that mitigate the weaknesses.
- An assessment of the likelihood, impact, and overall risk posed by the weaknesses.
- Recommendations.

This analysis shall be updated every year. The results of the risk analysis shall be considered confidential. This means that it will only be shared with non-HUBzero and non-RCHE staff on a need-to-know basis. Hard copies shall be kept in reasonably secure locations, and electronic copies shall not be available for public access.

No applications that access EPHI by means other than an SSH tunnel will be deployed on dash. Should the need arise for such an application, this policy will be revisited at that time.

B Risk Management

1. Goal: HUBzero will implement security measures designed to reduce the risks to EPHI to a reasonable level, provided that applications making use of EPHI are only accessed via SSH tunnel. HUBzero cannot alone provide a reasonable risk level for EPHI information without strong cooperation from the EPHI stakeholders and their considerable involvement in the risk management process.
2. Periodic Risk Management Process Requirements
   a. Assessment and prioritization, on the basis of risks, of EPHI Systems.

b. Selection and implementation of reasonable, appropriate, and cost-effective security measures to manage, mitigate, or accept identified risks.
c. Security training and awareness on implemented security measures to relevant workforce members.
d. Periodic evaluation and revision, as necessary, of the security measures.

3. Risk management process: The risk management process for dash.catalyzecare.org systems, excluding the EPHI-handling applications that use methods of access other than SSH, shall be conducted by HUBzero system administrators in consultation with the staff member most qualified with regards to security concerns, or by that staff member. The developers of applications handling EPHI information by means other than SSH tunnel need to perform their own risk management, and be aware of the risks involved with such means of access.
   a. Risk analysis: The risk analysis required by HIPAA (see 164.308 a 1 ii (A)) is a sound basis for risk management activities. Ticket handling is also a good opportunity to discover risks. Non-trivial issues can be discussed on the "ncn-maint" mailing list if it might help resolve the following steps. HUBzero staff will be available for consultation by developers of applications handling EPHI information.
   b. Risk prioritization: Risks identified in the risk analysis or otherwise shall be prioritized based on the overall calculated risk level. Amongst issues of equal level, potential impact to the dash server where the existing controls are the weakest and the expected cost of remediation is the lowest shall be used for prioritization. Risks at the highest level should be handled as soon as possible. Responsibility for responding to discovered risks should be passed to an appropriate staff member, e.g., by filing a ticket. Non-confidential, non-urgent risks and their solution can be discussed using the HUBzero Wish system.
   c. Method identification: The appropriate security methods to minimize or eliminate identified risks shall be identified. Security methods shall be identified based on the nature, feasibility, and effectiveness of the specific security method.
   d. Cost-benefit analysis: HUBzero shall identify and define the costs and benefits of implementing or not implementing the identified security methods.

e. Security method selection: Based on the cost-benefit analysis, HUBzero shall select the most appropriate, reasonable, and cost-effective security methods for reducing the identified risks.
f. Assignment of responsibility: HUBzero staff with the appropriate expertise shall implement the selected security methods.
g. Security method implementation: The selected security methods shall be properly implemented by the responsible workforce members.
h. Security method evaluation: The selected and implemented security methods shall be evaluated and revised, as necessary, by the HUBzero staff member most qualified with regards to security concerns.

4. Strategies for Managing Risk: The strategies for managing risk shall be proportionate with the risks to and sensitivity of EPHI. The security measures shall reasonably protect the confidentiality, integrity, and availability of EPHI. The following methods are used to manage risk:
   a. Risk acceptance-
   b. Risk avoidance-
   c. Risk limitation-
   d. Risk transference-
5. Results: The results of the risk management process shall be documented either in tickets, in the HUBzero wiki for the "production" group or in the software configuration management system's (currently "Ogre") comments and settings.

C Sanction Policy

Defaults as Purdue's policy.

D Information System Activity Review

1. Policy: HUBzero will review records of information system activity on a periodic basis. Additional reviews will be done as needed where incidents are reported or suspected. Information gathered from the system activity logs shall be filtered for events of interest, triggering an alert such as email to the system administrators directly or through a mailing list.
2. Procedure
   a. System administrators are responsible for the review of system activity, such as failed logins, failed access, and security incidents.
   b. Reviews shall be done at least once every regular business day. It is sufficient that a single system administrator does this, but it is OK to have more.

System administrators are responsible for coordinating this.

c. All system administrators must subscribe to the ncn-system mailing list, which contains log events triaged and filtered through the logcheck software. Only email accounts hosted on Purdue systems shall be used for subscribing to the list.
d. The audit standards shall be reviewed periodically and modified if indicated.
e. All system administrators shall be made aware of the audit standards.

a 2 Assigned Security Responsibility

Defaults as Purdue's policy

a 3 Workforce Security

(a) Background: HUBzero staff that have administrative rights or that otherwise have access for the purposes of performing activities covered by a business associate agreement ("privileged access") to the systems containing EPHI are covered by the following policies. That is because they could modify the system or application code that is used to store, process, transform, and/or modify EPHI and through that action expose the EPHI to unauthorized individuals. The exposure could be accidental (through a configuration change) or intentional (through modification of source code). For example, being root or having write access to directories where EPHI is stored means that they can potentially capture the unencrypted EPHI while performing activities permitted under a business associate agreement. Even after EPHI has been encrypted, the encryption key is available to people with this type of privileged access, so in effect they have full access. "Workforce member" below refers to HUBzero staff only.

(b) Authorization And/Or Supervision

(i) HUBzero shall ensure that HUBzero workforce members who have the ability to access EPHI or work in areas where EPHI might be accessed shall be properly authorized and/or supervised.

(ii) HUBzero will define and maintain processes for granting authorization and access to EPHI, including:

1. Procedure for permitting access to EPHI
2. Procedure for logging and tracking authorization of access to EPHI.
3. Procedure for reviewing and revising, on a periodic basis, authorization of access to EPHI (the periodic basis is to be defined in the documentation of that process).
4. The above are documented at 164.308 a 4 Information Access Management, Access Authorization.

(iii) Workforce members shall not be allowed access to EPHI or to areas where EPHI might be accessed until proper authorization is granted.

(iv) Only authorized workforce members who have need for privileged access in order to fulfill their respective job responsibilities shall be authorized to access EPHI or areas where EPHI might be accessed. HUBzero shall review access levels on a periodic basis and make revisions as necessary. HUBzero shall establish a procedure for reviewing and revising, on a periodic basis, authorization of access to EPHI or to areas where EPHI might be accessed.

(v) The above-mentioned procedure is documented at 164.308 a 4 Information Access Management, Access Establishment and Modification.

(c) Workforce Clearance Procedure

(i) HUBzero shall take reasonable and appropriate steps to ensure that workforce members have the appropriate authorization to access EPHI. See 164.308 a 4 Information Access Management, Access Authorization.

(ii) HUBzero managers, system administrators and the HIPAA liaison will work together to identify which HUBzero employees are allowed to grant privileged access to other workforce members or supervise them.

(iii) HUBzero will rely on Purdue University Human Resources to review prospective workforce members' backgrounds during the hiring process.

(d) Termination Procedures

(i) Workforce members leaving their position (whether or not they leave Purdue) must have their access privileges audited within one month of leaving.

(ii) The above audit must investigate group memberships, mailing list memberships, sudo privileges, public keys stored in the authorized_keys files of privileged accounts, "host" privileges visible in the user's page of the administrator interface of the hub, and any accounts stored in /etc/passwd files.

a 4 Information Access Management

(a) Definitions

(i) Privileged access to dash.catalyzecare.org is defined as having root or sudo access to the server or having permission to write to directories containing software codes that are used to operate upon EPHI consistent with duties permitted in a business associate agreement. In effect, this privileged access grants access to EPHI information.

(ii) Research access to dash.catalyzecare.org is defined as having non-privileged account access to directories that contain EPHI.

(b) Access Authorization

(i) Procedure for permitting privileged access to EPHI. The person granting privileged access must verify that the workforce member needs this access. The person granting privileged access must verify that the workforce member has taken the Purdue training and online exam, by consulting with the HIPAA liaison for ITaP Academic Technologies.

(ii) Procedure for logging and tracking authorization of privileged access to EPHI: Tracking authorization of privileged access to EPHI is done by gathering the list of users with established privileged access, as defined above. In other words, HUBzero uses the establishment of privileged access as a record of authorization.

(iii) Procedure for logging and tracking authorization of research access to EPHI: Tracking authorization of research access to EPHI is done by requiring each person requesting research access to complete a hard copy form indicating their identity and affiliation, the data to which they request access, approval by RCHE management, and approval by HUBzero's HIPAA liaison.

(iv) Procedure for reviewing and revising, on a periodic basis, authorization of access to EPHI.

1. Every year, an audit will verify if workforce members that were authorized still have their Purdue HIPAA certification and if they still need this access.

(c) Access Establishment and Modification

(i) Process for establishing, documenting, reviewing, and modifying access to EPHI

1. Procedure for establishing and documenting access to EPHI: This is done by granting privileged or research access as defined above, by the appropriate mechanism.
2. Procedure for reviewing on a regular basis workforce members' access privileges to EPHI: Every year, a list of which workforce members that have privileged access to systems with EPHI information will be made. Authorization will then be verified, and access privileges modified accordingly.
3. Procedure for modifying the access privileges of workforce members to EPHI, as appropriate, based on the periodic reviews: This is done by using the mechanism by which privileged or research access was granted, as described above.

(ii) Authorization and training of workforce members to access EPHI

1. Definition and classification of permitted access methods: Workforce members must use encrypted communication protocols (e.g., SSH) to access the systems and services for

which they have privileged access. Clear text protocols (e.g., MySQL, telnet) are expressly forbidden. Workforce members will be shown how to use SSH for tunneling clear text protocols, therefore encrypting the communication.

2. Definition and classification of length of time access will be permitted: Access will be permitted until a workforce member changes positions or an audit determines that their privileged access is not needed anymore.
3. Procedure for appropriate logging and tracking of activities by an authorized workforce member on EPHI: Activities of workforce members with privileged or research access are tracked the same on all HUBzero infrastructure regardless of whether EPHI is involved. HUBzero tracks logins via SSH.

a 5 Security Awareness and Training

(a) Security Reminders.

(i) HUBzero will post security reminders near the mailbox in Young Hall and send the same postings to RCHE to post in their offices in a location where impacted workforce will see them, reminding the workforce on the importance of protecting PHI.

(ii) Every time Purdue will release a quarterly HIPAA newsletter, an email will be sent on the "ncn-maint" mailing list and to people who have a current Purdue HIPAA certification, to remind people to read the newsletter. At the same time, the email will remind people of other Purdue security resources such as the SecurePurdue website.

(iii) At least one system administrator will be subscribed to debian-security-announce@lists.debian.org at all times, as long as we have Debian systems. The equivalent mailing list will be used for administrators of other operating systems.

(b) Protection From Malicious Software

(i) Practices and procedures for malware prevention and detection: The following practices and procedures are to be taught to system administrators. HUBzero infrastructure will be setup to automatically check for malware by using:

1. Intrusion detection software (e.g. rkhunter)
2. Anti-virus software (e.g. ClamAV)

(c) Malicious Software

(i) How to report malicious software

1. All events that may constitute IT Incidents should be reported to abuse@purdue.edu. More details on what constitutes an IT Incident and what to report are described in the Purdue Incident Response Policy.

(ii) How to recover from malicious software

1. Once an infection has been determined to have occurred, the infected system should be taken offline (shutdown) as soon as possible. The ongoing risks to other infrastructure

and users are a greater concern to HUBzero than the preservation of evidence achieved by examining the live system.

2. Malicious software can be extremely resistant to removal. Most often, wiping the hard drive, re-partitioning and complete OS installation from a trusted source is required, or is more effective than trying to fight the malware. The time necessary to decide whether this is required is often better spent in performing the procedure. However, HUBzero system administrators should attempt to determine the method by which the malicious software was installed. This is better done by looking at backups. Once a counter-measure has been determined, it should be applied to existing systems as well as to the rebuilt one as soon as possible.

(d) Training

(i) The previously described practices and procedures will be taught to HUBzero system administrators. This will be done by assigned reading of this wiki and discussion.

(e) Login Monitoring

(i) Given that dash.catalyzecare.org has been designed as a 24/7 research server; that accesses can presumably and justifiably occur at any time 24/7, and have been observed to occur at any time; that users include neophytes that often forget passwords and require many attempts for a valid login; that HUBzero workforce members have little knowledge of the habits of the clientele of the server; login discrepancies are extremely difficult to identify and any such identification is error-prone, HUBzero will not attempt to detect unauthorized access through login monitoring.

(ii) HUBzero's contribution to login monitoring will be limited to providing automated protection against password guessing attacks, by configuring and using the "fail2ban" software. System administrators will be taught to use fail2ban, and the configuration in use at HUBzero, from wiki pages and publicly available documentation on fail2ban.

(f) Password Management: This is addressed by Purdue policy.

a 6 Security Incident Procedures

Default as Purdue's policy.

a 7 Contingency Plan

(a) Disaster and emergency recovery strategy

(i) HUBzero does not prioritize the recovery of projects handling EPHI information over others. The HUBzero strategy aims at both preventing the need for recovery, and making a recovery possible even after very unlikely disasters. However, the speed of the recovery is not a primary consideration. Therefore,

HUBzero is only suitable as a hosting service for projects that have no Emergency Mode Operation requirements. HUBzero uses the following prevention techniques:

1. RAID (Redundant Array of Independent Disks)
2. UPS
3. Temperature monitoring software
4. Anti-virus software
5. Auditing and hardening software

(ii) The strategies for data protection aim to:

(iii) Provide daily images for up to 30 days

(iv) Have a recovery path for data up to one year old (best effort basis)

(v) Recover from single building-level disasters by having backups in a different building

(vi) Resist the failure of a backup technology by using two different technologies or two different backup service providers (in progress)

(vii) Recover from a Purdue-campus event-level disaster by having backups in a different part of the city or a different city (not currently implemented)

(b) Data Backup Plan

(i) Hubzero system administrators are responsible for monitoring backup operations at a system level. Applications handling EPHI data are responsible for providing HUBzero with files that can be backed up without race conditions, such as an encrypted database dump, and as opposed to a live database being updated while the backup is taking place. A spreadsheet is used to maintain the mapping of which hub is backed up by which servers or backup service providers. Backups are made daily using the following technologies and backup service providers, depending on the hub:

1. Dirvish (HUBzero): Dirvish uses rsync over SSH; all transport is encrypted. Snapshots are made daily and stored on disks. The backup servers are located on campus in a different building (HAAS or MSEE) from the hub machines (FREH), therefore lowering the risks due to an incident affecting a single building. Daily snapshots are kept for 30 days. Sunday weekly snapshots are kept for 3 months. Sunday monthly snapshots are kept for a year on the backup server. Any backup failures are automatically emailed to the mailing list "ncn-system", which is read by HUBzero system administrators and fixed by whoever is on duty. The inventory of the snapshots is available with a few simple UNIX commands on the appropriate backup server (e.g., "grep 'success' /backup/*/*/summary"). For each filesystem on each hub, all files are backed up except

temporary file systems (e.g., /tmp), virtual containers and mount points. Pascal Meunier manages Dirvish backups. For restoration, a ticket is created on HUBzero, and the appropriate files are securely copied to the requested destination using scp.

2. Symantec NetBackup (ECN): Symantec NetBackup is managed by Purdue University's ECN (Engineering Computing Network). Daily backups are made to tape in the MSEE building. Mid-level and partial dumps never leave the robot in MSEE 130. Full dumps are done twice a year and kept in the tape robot for a while. After all full dumps are complete, a copying operation is made to replicate the full dumps using transparent media-level encryption. These tapes are removed from the robot and stored in POTR. For restoration, a request is made to the ECN backup group at https://engineering.purdue.edu/ECN/Support/KB/Docs/RequestingBackups See http://www.purdue.edu/appservices/tsm.php
3. Bacula (HUBzero): Bacula is configured to provide daily incrementals, weekly differentials and monthly full backups. Data transport is done with TLS and host certificates, and tapes are stored in the HAAS building. This includes both client and server certificates, signed by HUBzero as a certificate authority and with the CA certificate being distributed ahead of time and out-of-band, therefore avoiding the concerns associated with self-signed certificates. Tapes are labeled with bar codes for reading by a tape library, and a number. The mapping between the tapes and contents is managed by the backup software. Tapes will be stored in the tape library. Tapes will be replaced whenever a write error will be detected on a particular tape — a different tape will be automatically used.
4. HP Data Projector is managed by Purdue's ITSO to perform backups using encrypted transport. Data storage is in the HAAS building. Purdue's management of backup solutions is documented at http://www.purdue.edu/appservices.

(c) Disaster Recovery Plan

(i) Conditions under which the Disaster Recovery Plan may be activated

(ii) Roles and responsibilities in executing the Disaster Recovery Plan

1. System administrators will be responsible for assessing further risks, the extent of the damage and steps needed to recovery or to prevent additional damage: Craig Van Tassle, Pascal Meunier

2. The project director will be responsible for coordinating the HUBzero response with other Purdue entities and other HUBzero staff: Diana Hancock
3. Michael Zentner will be responsible for contacting RCHE, and will need to be available for consultation

(iii) Recommended procedures

1. Actions to be taken to restore data, and to return systems to normal operations.
   a. Preparations
      i. Inventory, with IP addresses and DNS names, of all powered on computer hardware is kept on a host running ocsinventory (inventory software): inventory.hubzero.org. Powered off hardware is inventoried in a spreadsheet.
      ii. The network is configured as follows. Machines in the MATH building are on 128.46.18.0/24. Machines in MSEE 214 are on 128.46.17.0/24. Machines in FREH are on 128.46.19.0/24, 128.46.20.0/24, 128.46.21.0/24, and 128.46.22.0/25. 128.46.22.128/25 is used for VPN access through a Cisco 5520 firewall.
      iii. List of software licenses: SAS, STATA.

(iv) Order in which systems will be returned to operation.

1. Servers managed by HUBzero will be serviced in order of the total fees paid to HUBzero, starting with the largest. As of July 2012, this is servers hosting the following hubs: NanoHUB, PURR (research.hub.purdue.edu), NEES, HIPAA-level hubs, and starter hubs. In case of equality, servers identified by liaisons as having earliest high-profile calendar events or events critical for their funding and continuation will be restored first, provided the servers could be restored in time. For example, if server A has an event in two days, but the server can't be restored before 3 days and the event can't be delayed, then it will be passed over in favor of the next server having an event soon.

(v) Reporting and notification procedures

1. Please refer to Private Notification Information for additional phone numbers.
2. In the event of a disaster, the people to call are:
   a. Pascal Meunier 494-0855
   b. Craig Van Tassle 496-6413
   c. Samuel P Wilson 494-0667
   d. Noriemae (Nikki) Huang 494-0524
   e. Lynn Zentner 494-6742
   f. ELizabett Hillery 494-0840
   g. Michael J Mclennan 494-6495

h. Erich W Huebner 496-6640

3. For systems managed by ITSO, the "Unix on-call" should be contacted. The Purdue IOC will provide the exact, time-dependent, contact information. The Purdue IOC can be reached at 496-8200 for regular business and at 496-7272 for outage related calls.

(vi) Access Procedures: The Disaster Recovery Plan will specify how to obtain physical access to facilities, access to backup media, and access to the Disaster Recovery Plan. These are documented in 164.310 a 1 Facility Access Controls, Contingency Operations.

(vii) Test Procedures

1. The plan's primary copy will be this document. It will be updated every time personnel changes, and reviewed every year. It will be updated every time personnel changes, and reviewed every year.
2. The plan will be tested by calling all the numbers of the people that are to be notified, and asking them to access the plan on their USB key. The version on their USB key will be compared to the one on the document. Then, the staff will pretend that a fire happened in FREH, and will restore a server using facilities in another building.

(d) Emergency Mode Operation Plan: Emergency Mode Operation is not supported, and should not be applicable for applications handling EPHI on HUBzero managed servers. Therefore this requirement does not apply.

(e) Testing and Revision Procedures: HUBzero will take reasonable and appropriate steps to perform testing of its Contingency Plan to assess its sufficiency and determine whether it is accurate and up-to-date, and by making necessary revisions on an annual basis. The plan shall be revised whenever testing results indicate so, when roles and responsibilities of individuals change, and when there are significant changes to the hubs and the threats they face. Test procedures are documented in Test Procedures above.

(f) Applications and Data Criticality Analysis: No server is considered critical, and no server should be providing critical EPHI services. The prioritization is based on user base size and storage size, followed by hubs having high-profile calendar events or events critical for their funding and continuation.

a 8 Evaluation

Default as Purdue's policy.

b 1 Business Associates Contracts and Other Arrangements

Default as Purdue's policy.

164.310 Physical Safeguards – these default to those listed for the HUBzero HIPAA physical safeguards https://hubzero.org/groups/hubzero_hipaa/wiki

164.312 Technical Safeguards

a) Access Control

1. Unique user identification – each person having an account on dash, and such account is required to be unique to the user and not shared. Obtaining an account requires filling out an account request form, and having approval signatures from appropriate RCHE personnel and ITaP personnel managing the dash server. All database access accounts will also be unique, and named by the same process just described.
2. Emergency access procedure – does not apply because emergency access is not necessary given the intended use of the dash server.
3. Automatic logoff – dash accounts have an automatic logoff interval of 1 hour of inactivity.
4. File based project data storage and access
    a. Each authorized user of the dash server will have his or her own home directory. Home directory space on dash is very limited and should never be used to store EPHI or even deidentified derivatives of EPHI (hereinafter DD). The appropriate use for home directory space is for user created programs, SAS codes, and so forth that may compute based upon or manipulate EPHI or DD.
    b. Projects are organized within their own directories on dash (hereinafter "Project Directory"). All project directories are under the main directory /data/rcheprojects. For example, all data related to the safetynet project would be stored under /data/rcheprojects/safetynet.
    c. Each Project Directory has two subdirectories: businessassociate and researcher. The businessassociate subdirectory (hereinafter BASD) shall contain files that contain EPHI. The intended use of the BASD is to allow persons covered under a Business Associate Agreement (hereinafter BAA) to perform the data transformation or processing functions contemplated by the BAA. The BASD will at no point be made accessible to Researchers for the conduct of their research. Data that are not undergoing active work contemplated by a BAA will be encrypted using symmetric gpg encryption when at rest.
    d. The Project Directory "researcher" subdirectory (hereinafter RSD) may contain files that have both EPHI or that have been deidentified. A person acting as a Business Associate may place transformed or processed EPHI, or deidentified versions of EPHI (hereinafter Researcher Allowed Data, or RAD), into the RSD for access by researchers. Whether or not files in the RSD contain EPHI is governed by the Institutional Review Board determination of what researchers can access with respect to the project data. Each researcher may create their own subdirectory under the RSD for their subsequent

processing and research. It is intended that researchers do the work relative to a given project in the Project Directory that is specific for that project. For example, if a researcher r1 is authorized for two projects, p1 and p2, such researcher should create two different directories for their work on those projects: /data/rcheprojects/p1/researcher/r1 and /data/rcheprojects/p2/researcher/r1.

e. Access to the RSDs and BASDs will be implemented using the unix groups authorization method. A user can enter or leave a group only by the mechanisms defined in the dash policies regarding creation of accounts or review upon change of or departure from their position of employment.

f. As a general convention, a file that neither contains the three letters DiD in its name nor is contained in a directory path that has a directory named DiD in its path will be assumed to contain EPHI. Although for historical reasons there may be exceptions to this rule, it is expected that any new data arriving on the dash server will follow this convention. Therefore, researchers and business associates are expected to use the DiD convention when adding files to the dash server.

5. MySQL based project data storage and access

   a. The MySQL system may contain both EPHI and deidentified information. These two types of information shall not be stored in the same database. For those databases that contain EPHI, specific columns that contain the EPHI shall be encrypted.

   b. MySQL databases shall be authorized analogous to the group based access authorizations on the dash filesystem when such databases are directly accessible by users who have ssh access to dash.

   c. Any MySQL database that will be accessed by a program (External Program) whose function is to make that information or derivatives (hereinafter Extracted Information) thereof visible to individuals or computer systems outside of dash shall be accessed by a special account that is specifically authorized to access the MySQL database from a specified location. When accessing a database that contains EPHI, such special account will only be permitted to run a set of stored procedures. Such stored procedures are to provide the Extracted Information in a fashion usable by the external consumer of the data. In the event such Extracted Information will contain EPHI, the project involved shall have approved extraction of such information in its Institutional Review Board application. In the event that the Extracted Information does not contain EPHI, access to the External Program must be governed by authentication, but is not required to be ssh based authentication. For example, a

web server in a OpenVZ container on dash may be made generally accessible to the outside world if authentication is performed by standard web authentication mechanisms.

d. All External Programs, before being made accessible by someone who is not a developer of the External Program, should pass the IBM Appscan testing software.

b) Audit Control – this defaults to the HUBzero policies at https://hubzero.org/groups/hubzero_hipaa/wiki/164312bAuditControl

c) Integrity

1. Standard (Operational Requirements)
   a. Verification Procedures - Developers of applications hosted on dash must develop procedures for verifying that controls used to protect the integrity of EPHI are functioning appropriately.
   b. Response Procedures - Developers of applications hosted on dash should develop procedures for detecting attempts to modify or destroy EPHI by attacking the application. HUBzero will attempt to detect system-level attacks as described in the other technical safeguard sections (164.312). HUBzero's response to successful unauthorized modification or destruction of EPHI is to restore data from the last backup, if available (see Contingency Plan). Moreover, HUBzero and developers of applications will respond according to the Purdue Incident Response Policy (seehttp://www.purdue.edu/policies/pages/information_technology/info_tech.html).
2. Implementation (Operational Specifications) - The hosted applications must implement their own protection scheme (e.g., foreign key constraints) to protect EPHI information.

d) Person or Entity Authentication

Purdue has related standards:

1. Authentication and Authorization Policy:http://www.purdue.edu/policies/pages/information_technology/v_1_2.html

2. User Credentials Standard:http://www.purdue.edu/securepurdue/bestPractices/passStandards.cfm

3. Access Controls Standard:http://www.purdue.edu/securepurdue/bestPractices/accessControlStandards.cfm

ITaP verifies people are who they say they are by requiring the account request form to be submitted in person to RCHE and ITaP staff prior to an account being created on dash. The authors and managers of covered applications must provide their own mechanism to verify that the people who registered the account are who they say they are.

d) Transmission Security – defaults to HUBzero policy at https://hubzero.org/groups/hubzero_hipaa/wiki/164312dTransmissionSecurity