PERFECT HUMAN FUNCTION

HIPAA Privacy and Security Policy and Procedures

I. Assignment of HIPAA Privacy/Security Officer

Melissa Zitt has been designated as our HIPAA Officer by Dr. Patrick Zitt and Perfect Human Function and has authority to establish, implement, and enforce these policies and procedures for the security and privacy of our patients protected health information (PHI).

II. Risk Assessment

HIPAA Officer is responsible for conducting annual HIPAA privacy and security risk assessment. The assessment will be completed with the assistance of at least two other employees.

Additional risk assessments may be necessary each time (1) new software or hardware is acquired and placed in service; (2) when a new service or procedure is initiated; (3) when there is a significant change in an existing service or procedure; or (4) when there is a change or addition to the physical layout of our office.

The HIPAA Officer will periodically but at least quarterly review the DHHS's HIPAA website to determine if there have been any changes in the HIPAA rules and regulations and to determine if any changes or modifications to this policy and procedure is necessary due to changes in HIPAA rules, regulations or regulatory interpretations.

[See Addendum IV for sample risk assessment form]

III. Policy regarding physical access to building

Entrance to our facility is kept locked at all times.

Employees access our office via main entrance which is unlocked only via key. Facility is not accessible by anyone other than employees or other authorized personel.

IV. Policy regarding confidentiality of all forms of PHI

All PHI regardless of its form, mechanism of transmission, or storage is to be kept confidential. Only individuals with a business need to know are allowed to view, read, or discuss any part of a patient's PHI. During initial new hire orientation and at annual HIPAA training employees are reminded that any viewing, reading, or discussions of PHI that is not for business purposes is prohibited. An employee who violates this confidentiality policy will be subject to sanctions up to immediate termination. All employees are required to verify in writing that they have read and will comply with our policy regarding confidentiality of all forms of PHI.

V. Policy regarding security of electronic PHI (e-PHI)

Employees whose job functions require access to our computer system will be given a secure, unique password to access the system. Passwords will consist of at least five characters, upper and lower case, alpha numeric and shall be changed at least every 90 days.

Access will be immediately terminated for employees who leave our employment.

All PHI transmitted to third parties will be transmitted on secured lines. The security of transmission lines will be verified via contract with third party responsible for transmitting our patient's PHI.

No digitally stored PHI shall leave this facility without being first encrypted; this includes laptops, flash drive devices, CDs, and e-mail.

VI. Patient request for accounting of all disclosures made by Perfect Human Function.

Patients have a right to request an accounting of all disclosures of their PHI made by Perfect Human Function. When a patient makes such a request, Melissa Zitt will be notified. The patient will be told when the information will be available and given the option of waiting or returning to pick-up the data.

VII. Patient request for restriction of PHI paid for "out of pocket"

Patients who pay for a procedure, test, or service out of pocket (fully paid for by patient with no reimbursement or additional payment by a third party),

have a right to have all information regarding such procedure/test held confidentially and not released to third parties. To exercise this right the patient must (1) pay for test/procedure and (2) make known to Perfect Human Function their desire to have information regarding the procedure/test held in confidence and not released to third parties. Any employee who receives such a request must immediately inform Melissa Zitt who will flag the information as being restricted.[1] HIPAA allows for the release of restricted PHI (1) in compliance to a subpoena; (2) in compliance to statutory reporting requirement; or (3) upon receiving an unrestricted, HIPAA compliant authorization for release of medical records from the patient, patient's legal representative, or executor of deceased patient's estate.

VIII. Policy regarding charges for e-copies of medical records

The Privacy Rule permits the Covered Entity (a healthcare provider) to impose reasonable, cost-based fees for paper copies (See Addendum I, page 5).

According to HITECH the covered entity may charge for the labor cost of making the e-copy. This does not include the cost for searching the data base to find appropriate medical record(s). Currently (October 1, 2010) there is no guidance regarding whether the covered entity is allowed to charge for the cost of the media on which the e-copy is provided to the patient - i.e., CD, flash drive, etc.

IX. Business continuity

Should the facility come under attack or suffer from an act of God, all records may be accessed from our off site server. Business will continue as usual.

X. HIPAA Incident/Breach Investigation

Any incident in which the privacy/security of a patient's PHI may have been compromised will be immediately reported to Melissa Zitt. An incident investigation will be initiated without unreasonable delay. The HIPAA Officer will establish an Incident Response Team (IRT) to investigate incidents and determine if the incident rises to the level of a breach. Refer to definition of

[1] This contemplates development and implementation of appropriate software programming with your electronic medical records (EMR) vendor.

IRT in Addendum II, page 7. The procedure for conducting HIPAA incident/breach investigation is located in Addendum II, pages 10-12.

XI. Sanction Policy

All employees will receive training regarding Perfect Human Function's policy for sanctioning employees who violate our HIPAA privacy/security policy. Employees shall receive training prior to assuming work duties and annually thereafter.[2] Perfect Human Function's HIPAA sanction policy is located in Addendum III, pages 15-16.

XII. Document Retention Policy

a. All HIPAA documentation such as policy and procedures, risk assessment, incident investigation, breach notification, and training records will be maintained for at least six years[3] in our HIPAA records and documentation.

[2] Note: HIPAA requires "periodic" training but does not specify the time frame—annually is recommended by most HIPAA Officers.

[3] Standard (Documentation) (Time Limit) Sec. 164.316(b)(2)(i)

Addendum I

HIPAA FAQs

>www.hhs.gov/ocr/privacy/hipaa/faq<

If patients request copies of their medical records as permitted by the Privacy Rule, are they required to pay for the copies?

Answer:

The Privacy Rule permits the covered entity to impose reasonable, cost-based fees. The fee may include only the cost of copying (including supplies and labor) and postage, if the patient requests that the copy be mailed. If the patient has agreed to receive a summary or explanation of his or her protected health information, the covered entity may also charge a fee for preparation of the summary or explanation. The fee may not include costs associated with searching for and retrieving the requested information. See 45 CFR 164.524.

Date Created: 12/20/2002
Last Updated: 03/14/2006

[Accessed 9/22/2010 RK]

Addendum II

Perfect Human Function

HIPAA Incident/Breach Investigation Procedure

I. Purpose

To distinguish between (1) cases in which our HIPAA policy was not correctly followed but such violation did not result in the unauthorized release of protected health information (PHI) (referred to as a HIPAA incident) and (2) cases involving the unauthorized release of PHI and said release resulted in or is reasonably expected to result in financial, reputational or other harm to the patient. This investigation procedure outlines the process for contacting the patient and identifying risk management measures to mitigate identified risks.

II. Definitions

Breach is the unauthorized acquisition, access, use or disclosure of PHI in a manner not permitted by HIPAA regulations which compromises the security or privacy of the PHI and poses a significant risk of financial, reputational, or other harm to the patient except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. (Also see definition of incident and reportable breach).

Breach Notification is a HIPAA requirement in which the Covered Entity (CE) that has experienced a breach must notify the patient that the privacy or security of their PHI has been compromised.

Business Associate (BA) is a business organization but not an employee of the CE that performs or assists in the performance of activity involving the use or disclosure of individually identifiable health information; for example, claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management or practice management.

Commercial Supplier (CS) is a business organization that provides services to a CE. While said services do not require CS to directly handle or impact PHI, their presence in the CE's facility may cause or allow them to come in contact with PHI. A janitorial service is an example of a commercial supplier.

Commercial Supplier agreement is a signed contract or memo of understanding between the CE and commercial supplier explaining the CS's duty to avoid PHI and provides assurances that the CS will instruct their employees regarding their duty to avoid viewing, reading, copying or otherwise obtaining information relating to patients PHI.

Covered Entity (CE) is a healthcare provider, a health plan, or a healthcare clearinghouse.

e-PHI is individually identifiable patient healthcare information created, stored or transmitted in electronic format.

Health Information is any information, whether oral or recorded in any form or medium, that: (1) is created or received by a healthcare provider, health plan, public health authority, employer, and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual.

HIPAA Officer is the individual formally assigned the duty to establish, implement, and monitor the CE's HIPAA policy and procedures. In small CEs both the Privacy and Security regulations could be handled by one individual, whereas in a large CE one individual may be assigned as the CE's HIPAA Privacy Officer and a second individual assigned as the CE's HIPAA Security Officer.

Incident is an actual or suspected unauthorized release, loss, or destruction of PHI but upon complete investigation it is determined by the Incident Response Team that the incident does not represent a significant risk of financial, reputational, or other harm to the individual.

Incident Response Team (IRT) is composed of members of the CE's staff including at least one key individual with decision making authority. The team is responsible for investigating the actual or suspected unauthorized access, release, or destruction of PHI; making the determination as to whether or not (1) the incident did in fact occur, (2) whether or not the incident rises to the level of a breach, (3) identifying appropriate Risk Management interventions to prevent similar re-occurrence, (4) assuring appropriate individuals are notified, and (5) assuring appropriate reports are made to Department of Health and Human Services (DHHS) when breach occurs.

Individually Identifiable Health Information any protected health information about an individual that can possibly be used to identify that individual and connect him/her to the health information.

Notification the contacting of individual(s) (or if deceased-next of kin or executor of estate) who is the subject of the unauthorized disclosure, release, loss or destruction of their PHI. Notification is required when the incident is determined to rise to the level of a breach.

Office of Civil Rights (OCR) is the Federal agency authorized by DHHS to investigate claims of HIPAA Privacy or Security breaches.

Protected Health Information (PHI) individually identifiable health information created, transmitted or maintained by CE or BA that (1) identifies the individual or offers a reasonable basis for reconstructing said identity, (2) is created, received, maintained or transmitted by the CE or BA, and (3) refers to a past, present or future physical or mental condition, healthcare treatment, or payment for healthcare.

Reportable Breach is a HIPAA incident that rises to the level of a breach. A HIPAA breach requires the CE to notify the patient, log the breach and report all such breaches to DHHS annually—If 500 or more individuals are involved in a given breach then special notification/reporting requirements apply.

Risk Analysis is the process by which the CE attempts to (1) identify all ways in which an unauthorized release, loss, access, or destruction of PHI could occur; (2) determine what risk management protections are currently in place to minimize the likelihood of the identified risk occurring; (3) assess the current level of risk management protections for each identified risk; (4) recommend additional privacy or security safeguards as needed; (5) review DHHS's website for breach events at other CEs that might suggest weaknesses in CE's privacy/security safeguards; and (6) assess adequacy of HIPAA training for CE's staff.

Sanction Policy is CE's written employee disciplinary policy that outlines the consequences of an employee's violation of the CE's HIPAA Privacy and Security policy and procedures. The sanction policy clearly states that the CE retains the right to immediately terminate an employee for what the CE determines to be an egregious violation of the CE's HIPAA Privacy or Security policy/procedures.

Unsecured PHI is PHI that is not secured through the use of a technology or methodology specified by HIPAA/HITECH rules or regulations. Generally it would be e-PHI not secured by encryption, paper or other media containing PHI that has not been shredded or destroyed in a manner that would prevent it from being reassembled.

III. Acquiring Knowledge of Actual or Suspected Breach:

There are many ways in which we may become aware of an actual or suspected breach.

1. Employee training is a major key to the early discovery of a suspected or actual breach. Early detection will often prevent an incident from becoming a reportable/notifiable breach. As part of employee HIPAA training all employees will be instructed to report any actual or suspected breach to the HIPAA Officer as soon as it is discovered or suspected.
2. Business Associate may cause or become aware of a breach and inform us.
3. Another CE may become aware of an actual or suspected breach and inform us.
4. The patient may become aware of an actual or suspected breach and inform us.
5. We may discover an actual or suspected breach while performing an audit of our HIPAA privacy/security policy and procedures.
6. We may be informed by the Office of Civil Rights that a complaint has been filed against us.

Perfect Human Function will investigate all incidents we become aware of to determine if a breach did in fact occur; to determine steps necessary to mitigate possible damage to patient; to determine risk management interventions necessary to prevent such incidents from reoccurring; and, to provide appropriate notification to patient and report to Department of Health and Human Services (DHHS).

IV. Unsecured PHI—Exceptions & Safe Harbors

HIPAA allows for two **exceptions** and three **safe harbors** for the unauthorized release of PHI in which breach notification is not required. The following **exceptions** are allowed:

(1) when unauthorized access or use of PHI is unintentional and is made by an employee working within the scope of their job in which they would normally be expected to access or use PHI and such access is not continued, enlarged or disclosed by said employee; and

(2) an unintended or accidental disclosure is caused by an employee who is authorized to access, use or disclose PHI at the facility in which they work (our employee) who sends or causes to be sent PHI to another individual in another healthcare facility who is also authorized to access, acquire or use PHI at their facility (an employee of another healthcare facility or other CE) provided the second employee agrees to return or destroy PHI and agrees not to disclose or further access PHI.

The three **safe harbors** are:

(1) The unauthorized release of e-PHI but the e-PHI is protected by encryption;

(2) The media on which the PHI was stored has been destroyed: (a) paper, film or hard copy media destroyed via shredding, incineration or, for digital/video media, destroyed in such a manner that the PHI cannot be reconstructed (For example; cutting CD into small parts), (b) electronic media destroyed or rendered un-retrievable in a manner consistent with NIST Special Publication 800-88, Guide to Media Sanitization; or,

(3) The unauthorized release consisted of health information that was completely de-identified—removal of all names, addresses down to zip code, social security numbers, date of birth, phone numbers, case numbers or any other data that might be used to trace back and identify the individual.

Unauthorized releases that fall under these exceptions or safe harbors are not considered as a breach and do not require notification of patient or reporting to DHHS.

V. Incident Response Team (IRT):

[Replace with name of your organization] has established an Incident Response Team and charged it with the responsibility of investigating HIPAA incidents. The team is composed of at least one key decision maker, i.e., an individual who is authorized by the organization to make key decisions relative to organizational policy and expenditure of organizational funds, and at least two employees one of whom has line (as opposed to management) responsibility. The following individuals are members of Perfect Human Function's Incident Response Team:

1. Patrick Zitt [Key Decision Maker]
2. Melissa Zitt [HIPAA Officer]

VI. Procedure

Distinguish between a HIPAA incident and a breach. Breaches of PHI would require notification of patient and inclusion in the annual report to DHHS. If breach involves 500 or more individual patients then DHHS must be immediately notified and public news media must be advised.

1. First determine if the incident/breach falls within one of the exceptions or safe harbors allowed by HIPAA
    i. If Yes, document and close file
    ii. If No, move to # 2.

2. Second determine if there has been an impermissible use or disclosure of PHI under HIPAA rules.

    i. If No (there has not been an impermissible use or disclosure of PHI), document rationale and close file. For example, the incident falls under the “Oops!” category or a case in which the individual would not reasonably be able to retain the PHI, such as a visitor glancing at a computer screen containing PHI.

        1. Documentation should include date, time and names of Incident Response Team members as well as a brief description of the incident and the reason it was determined the incident was not an impermissible use or disclosure of PHI under HIPAA rules. Include any FAQ from DHHS’s website that was used to support final decision as well as citation to any HIPAA rules or regulations used to make the determination.

        2. Refer to XI, page 14, Note Regarding Determination of Incident vs. Breach

    ii. If Yes, move to 3.

3. Third, determine if the impermissible use or disclosure compromises the security or privacy of the PHI, i.e., there is a significant risk of financial, reputational, or other harm to the individual.

    i. If No (this was an incident that did not rise to the level of a breach), document your rationale, record this as a HIPAA incident, and close file.

        1. Documentation should include date, time and names of Incident Response Team members as well as a brief description of the incident and the reason it was determined the incident was not an impermissible use or disclosure of PHI under HIPAA rules. Include any FAQ from DHHS’s website that was used to support final decision as well as citation to any HIPAA rules or regulations used to make the determination.

        2. Determine and document why our policy, procedures, or training failed to prevent this incident and what risk

management intervention(s) was taken to prevent similar occurrences.

3. Include this incident in our annual risk assessment for ongoing review and monitoring.

4. If changes were made to office policies or procedures as part of risk management intervention subsequent to incident, train all employees, owners, and business associates as needed and document training.

5. Refer to IX, page 14, Note Regarding Determination of Incident vs. Breach

ii. If Yes (Breach did occur)

1. Complete investigation as soon as possible

2. Determine cause of breach—why our HIPAA policy and procedures failed to prevent the breach from occurring, not just who caused the breach. For example: Breach occurred due to failure to follow procedure arising from failure to train employee before assigning her to job; failure of BA to follow BA agreement; or failure of computer firewall due to outdated technology.

3. Identify corrective action(s) (risk management interventions) to be taken to address failure(s) including sanction for employee(s) if appropriate.

4. Notify patient as per VII below

5. Log breach for end of year reporting to DHHS

6. Include failure in annual risk assessment

VII. Notification of Patient

When the Incident Response Team determines that there has been an unauthorized disclosure of a patient's PHI, and it rises to the level of a breach, then the patient must be notified. Notification will be made as soon as the determination of an unauthorized disclosure is made and appropriate investigation has been completed, but no later than 60 days from discovery. It is expected that the notification will be completed as soon as possible - once discovery and appropriate investigation is completed the notification will be made at that time without waiting for the running of the sixty day maximum limit. In

addition, if the situation is deemed urgent by the Incident Response Team, notification to the patient will be made immediately without waiting for full investigation. Urgent notification will be made, if possible, via phone. Non-urgent notification will be provided as follows:

1. Written notification provided via first class mail with copy of letter placed in patient's medical record. Said notification mailed to last known address. If patient has given prior approval for communication via e-mail then notification may be made via e-mail. Additional mailings may be required as additional information is obtained.

2. If individual is deceased then notification will be mailed to next of kin or executor of estate.

VIII. Business Associate Notification

If a Business Associate (BA) becomes aware of a breach caused by the BA, our written BA agreement requires the BA to notify us immediately. Our Incident Response Team will conduct the investigation to determine if impermissible disclosure occurred, how to notify the patient, and what steps should be taken to prevent similar incident/breach from reoccurring.

IX. Delay of Notification Requested by Law Enforcement

Notification may be delayed if law enforcement official determine that notification would impede a criminal investigation or endanger national security. The delay request must be in written form and identifies the law enforcement official making the request. The delay can be for no more than 30 days unless a written request for a specific extension is made within the initial 30 day extension by a law enforcement official.

X. Elements of the Written Notification

The patient's written notification of a breach involving their PHI will contain:

1. A short description of how the breach occurred; when it occurred; when we discovered the breach

2. An explanation of the type of PHI involved in the breach such as patient name (full or partial), diagnosis, treatment, lab/test results, social security number, date of birth, patient's address, account or case number and/or financial data such as credit card numbers

3. Our recommendation(s) to the patient as to the steps he/she should take to protect themselves from identity theft or the unauthorized use of their medical insurance accounts

4. An explanation of what we are doing to prevent re-occurrence of such breaches

5. Information the patient may use to contact us if they have further questions

XI. Note Regarding Determination of Incident vs. Breach

If, after an appropriate investigation has been conducted, it is determined that the incident did not rise to the level of a breach, we have the burden of proof, i.e., we must be able, if required at a later time, to demonstrate to DHHS or OCR that the impermissible use or disclosure did not constitute a breach, and therefore we were not required to notify the patient and include incident in our annual report of breaches to DHHS. Appropriate documentation of the investigation and the rationale used to make our non-breach (incident) determination will be maintained for at least six years after the initial non-breach finding. To demonstrate due diligence regarding our desire to comply with HIPAA requirement, we will document all changes in policies/procedures and/or additional staff training that resulted from our investigation into the incident. We will also include the incident in our annual risk assessment.

Addendum III

Perfect Human Function

HIPAA Privacy and Security

SANCTION GUIDELINE

Legal and Ethical Duty

Healthcare providers, employees, consultants, business associates and others who have a business reason to create, maintain, view, or transmit confidential data relative to patient's medical care have a legal and ethical duty to maintain the privacy, security and confidentiality of such medical information. Violation of this duty will result in sanctions being imposed on the responsible party.

Federal Privacy and Security Legal Requirements

Perfect Human Function requires all employees, as a condition of employment, to receive training regarding their responsibility relative to HIPAA privacy and security standards. All employees must follow established privacy and security policies to ensure the confidentiality, integrity, and availability of all protected health information. All individuals having access to protected health information (PHI) are required to read, sign, and comply with this organization's privacy and security policy. By signing the privacy and security policy employee acknowledges that both Perfect Human Function and the employee have a legal duty to comply to the best of their ability with the privacy and security policy.

Sanctions for Breach of Privacy and Security Policy

An employee(s) who, without a business "need to know," unintentionally or carelessly views or accesses PHI is subject to an initial verbal warning. This warning is given with an additional warning that repeat of this or similar offense will result in further disciplinary action not to exclude suspension without pay or immediate termination of employment.

An employee(s) who, without a business "need to know," unintentionally or carelessly views or accesses PHI and then relates portions of the PHI to another individual is subject to an initial written warning. This warning is given with an additional warning that repeat of this or similar offense will result in further disciplinary action not to exclude suspension without pay or immediate termination of employment.

An employee(s) who, without a business need to know, intentionally views or accesses PHI to satisfy personal desire to learn details regarding a patients PHI is subject to immediate termination of employment.

An employee(s) who views or access PHI with malicious intent or desire for personal gain is subject to immediate termination of employment.

Non Retaliation Policy

An employee who, in good faith and belief that a privacy or security policy has been violated, reports such concern to Perfect Human Function HIPAA officer shall not be subject to retaliation, harassment, or intimidation as a result of such communication to HIPAA officer. Should such an employee believe he/she is being harassed by Patrick Zitt.

Date Policy Created/Approved May 13, 2017

Date Policy Reviewed/Revised _____

Date Policy Reviewed/Revised _____

Date Policy Reviewed/Revised _____

Date Policy Reviewed/Revised _____

Date Policy Reviewed/Revised _____

Addendum IV:

Risk Assessment Form (Example)

Scoring:

0 = Probability – possible, but not likely
1 = Probability - could happen
2 = Probability - likely to happen, but not guaranteed to happen

	Risk	Probability of Occurrence
1	Lost laptop (MD takes unencrypted laptop home)	1
2	Lost paper medical record (Nurse puts lab reports in pocket and waits until end of day to file reports)	2
3	Hacker getting into our system and obtaining e-PHI	1
4	Lost CD or flash drive (MD takes unencrypted flash drives home)	2
5	Break-in and patient records stolen (Facility specializes in pain management and is located in a high crime area)	2
6	Patient's HIV prescription accidentally broadcast to dozens of fax numbers in the system	0

1. Begin with blank spreadsheet or flip chart and have Risk Assessment Team brainstorm all the possible ways in which the confidentiality of PHI might be breached.
2. List each risk under the risk column, and then as a group assign the probability of the risk occurring at our facility. The brainstorming session should be free-flowing, no bad ideas, be careful that an authority figure does not repress the free flowing of ideas.
3. Take all the "2s" and develop risk interventions that will eliminate or reduce the possibility of the risk occurring. For example; under risk number 2 a policy could be established that all lab reports are filed as soon as they are received; risk number 4 could be reduced to a "0" with the adoption of encryption technology for CDs and flash drives used in the facility; and, risk number 5 could be lowered to a "1" with the addition of better lighting and a monitored security service.

4. Risk number 6 was scored a “0” because the Office Manager had the broadcast function removed prior to putting the software into service.

5. Keep documentation of the meeting to use as a beginning point for next years session; check DHHS’s HIPAA web site to determine if other facilities have had breaches that might occur in our facility; perform risk assessment each time new or updated electronic medical records software/hardware is adopted; perform risk assessment any time a new procedure or new clinical technology is adopted; and maintain documentation for at least six years.

6. Keep in mind that the purpose of Risk Assessment is to (1) identify potential risk to PHI, (2) set the priority for addressing identified risks, (3) establish risk management interventions to minimize or eliminate identified risks, (4) test our current risk management interventions to make sure they are still appropriate, and (5) gauge the effectiveness of our HIPAA training.