Title: Confidentiality of Protected Health Information	
Policy Area: Compliance	Owner: John McDowell, Director of Governance and Compliance
Date of Approval: Approval By: Appropriate Committees	10/19
Original Date: Revision Dates: Reviewed with no Changes Dates:	10/19 X/XX; X/XX X/XX; X/XX
Signature:	

I. Title: Confidentiality of Protected Health Information

II. General Statement of Purpose:

The purpose of this policy is to establish general requirements for protecting the confidentiality of Protected Health Information ("PHI") while allowing its necessary use, access and disclosure for purposes of providing high quality care to the patients of Wellfound Behavioral Health Hospital.

Additionally, the purpose of this policy is to establish standards for requesting, modifying, and terminating access to Wellfound Behavioral Health Hospital's information technology data.

III. Scope:

This policy applies to all members of the Wellfound Behavioral Health Hospital workforce including, but not limited to: employees, medical staff, volunteers, students, administrative staff, and other persons performing work for or at Wellfound Behavioral Health Hospital.

IV. Policy:

All PHI, in any format (oral, written, or electronic), produced by, or on behalf of, Wellfound Behavioral Health Hospital, is confidential and must not be shared by employees and/or agents of Wellfound Behavioral Health Hospital with other individuals and entities, including other Wellfound Behavioral Health Hospital employees and/or agents, unless necessary in order to enable the employee or agent to perform the duties within the scope of his or her employment. This policy is subject to limited exceptions as outlined below.

In general, all PHI, in any format, produced by or on behalf of Wellfound Behavioral Health Hospital, is also subject to the Minimum Necessary Rule when said PHI is being accessed, used or disclosed, unless the access, use, or disclosure falls under a limited set of exceptions as outlined below.

It is Wellfound Behavioral Health Hospital's policy to determine the need for access to, and appropriate levels of security to protect the confidentiality of data on our systems, including Electronic Protected Health Information (ePHI). Wellfound Behavioral Health Hospital's personnel shall be identified and categorized by the degree of access to and need for patient health information.

V. Definitions:

Authorization: An individual's signed permission that allows a covered entity to use or disclose the individual's PHI for the purpose(s), and to the recipient(s), as stated in the Authorization.

Business Associate: An entity that performs, or assists in the performance of, a function or activity involving the access, use or disclosure of PHI, including, but not limited to, claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, or re-pricing.

Covered Entity: A facility that conducts Health Care Operations involving the creation and transmission of PHI. Each facility in Wellfound Behavioral Health Hospital which conducts Health Care Operations is its own Covered Entity. These Covered Entities are collectively considered an Organized Health Care Arrangement which allows each of the included Covered Entities to share PHI for Treatment, Payment and Health Care Operations.

Department Director: The person with managerial responsibility for an identified Wellfound Behavioral Health Hospital Department.

Disclosure: The release, transfer, access to, or divulging of information in any other manner outside the entity holding the information.

Health Care Operations: Activities of a Wellfound Behavioral Health Hospital facility as they relate to covered functions, including, but not limited to, quality assessment and improvement activities, reviewing the competence or qualifications of health care professionals, activities related to contracting for health insurance or health benefits, conducting or arranging for medical review, legal review, or auditing functions, business planning and development, and business management and administrative activities.

Protected Health Information or "PHI": Any oral, written or electronic individually identifiable health information collected or stored by a facility. Individually identifiable health information includes demographic information and any information that relates to the past, present or future physical or mental condition of an individual. The Health Insurance Portability and Accountability Act ("HIPAA") details eighteen items that render PHI identifiable:

1. Names;
2. Geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code in certain situations;
3. All elements of date (except year) for dates directly related to an individual, including birth date, discharge date, date of death; and all ages over 89 and all elements of dates indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers;
13. Medical Device Identifiers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code.

Payment: The actions taken by a health care provider or health plan to obtain or provide reimbursement for the provision of health care.

Treatment: The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party, consultation between health care providers relating to a patient, or the referral of a patient for health care from one health care provider to another.

Minimum Necessary: The minimum necessary standard, a key protection of the HIPAA Privacy Rule, is derived from confidentiality codes and practices in common use today. It is based on sound current practice that protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. The Privacy Rule's requirements for minimum necessary are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity.

IV. Procedures/Guidelines:

A. Confidentiality of PHI
   1. To protect the confidentiality of PHI, individuals included within the scope of this policy should not access, discuss, or share PHI in public areas or with any individuals who do not have a need to know the information for purposes such as treatment, payment, health care operations or as otherwise required or permitted by law.

B. Special Categories of PHI with heightened Protection
   1. The Following categories of PHI and Heightened privacy protection:
      i. HIV/AIDS PHI (See Wellfound Behavioral Health Hospital Policy #800.52);
      ii. Mental health-related PHI (See Wellfound Behavioral Health Hospital Policy #800.53);
      iii. Substance abuse (Drug and Alcohol) PHI (See Wellfound Behavioral Health Hospital Policy #800.55);
      iv. Psychotherapy notes (See Wellfound Behavioral Health Hospital Policy #800.02);

C. Obligation to Sign Confidentiality of Wellfound Behavioral Health Hospital Information Attestation and Agree to Access and Confidentiality User Agreement
   1. All individuals within the scope of this policy are required to sign the "Confidentiality Statement and Attestation.
   2. Business Associates providing services on behalf of Wellfound Behavioral Health Hospital are required to sign a Business Associate Agreement. A review will be performed by The Corporate Compliance Officer to confirm Business Associate Agreements are in place as appropriate on a periodic basis.

D. Obligation of Department Directors
   1. It is the responsibility of each Department Director to evaluate the PHI generated and received within his or her Departments. It is then the responsibility of each Department Manager to develop and implement reasonable policies and procedures to safeguard all PHI and determine the categories of individuals within the Department who must have access to PHI to accomplish their employment duties.
   2. It is the responsibility of the Department Director to ensure that only those necessary individuals attend medical education conferences in which PHI is discussed. At all such medical education conferences, any reference to the identity of patients shall be redacted from the case presentation. The case will be given a fictitious name or de- identified number that will be used throughout the discussion but will not be Associated with the patient's PHI in any way.

E. Access, Use, or Disclosure of PHI Permitted without an Authorization
   1. Wellfound Behavioral Health Hospital is only permitted to access, use, or disclose an individual's PHI for treatment, payment or health care operations, unless a validly executed "Authorization for Release of Protected Health Information" form has been provided, or a specific regulatory exception applies.
   2. An Authorization to access, use or disclose PHI is not required, but may be requested for record- keeping purposes, in the following circumstances:
      i. The access, use, or disclosure involves the patient, the patient's personal representative), or a patient's family member or friend who, according to the health care provider's professional judgment, is acting in the best interest of the patient's care;

ii. The access, use, or disclosure involves a correctional institution or other law enforcement custodian who is overseeing the health care of an incarcerated patient, for purposes of caring for the patient, in addition to the others in the institution;
iii. Patient's will be given the option to allow individuals to know of their treatment at Wellfound Behavioral Health Hospital through the assignment of a code.
iv. The access, use or disclosure is for purposes of emergencies, national security and intelligence activities, military or veteran's affairs activities, public health, regulatory oversight, or accreditation; is in accordance with a legally valid subpoena; or is permitted or required by law;
v. The access, use or disclosure is to a medical examiner or funeral director for purposes of carrying out their scope of duties related to the patient;
vi. The access, use or disclosure is for the purposes of cadaveric, eye, or tissue donation if that is consistent with the patient or patient's designated representative's intent; and/or
vii. The access, use or disclosure is legally required by a program providing benefits to a patient for a work-related injury or illness.

Individuals have the right to request restrictions on the access, use or disclosure of their PHI

F. The Minimum Necessary Rule
1. In general, when permissibly accessing, using or disclosing PHI, Wellfound Behavioral Health Hospital must limit such access, use or disclosure to the minimum necessary to accomplish the intended purpose of the access, use or disclosure.
2. For guidance on determining the minimum necessary amount of information to accomplish an intended purpose in any particular case, please contact the facility Privacy Officer
3. When the Minimum Necessary Rule Does Not Apply - the minimum necessary standard does not apply in the following circumstances:
    i. The PHI is for use by, or a disclosure to, a healthcare provider for treatment purposes;
    ii. The disclosure is to the patient or the patient's legally authorized representative (this is limited to the extent that such individual is authorized to receive such information);
    iii. The disclosure is pursuant to a valid authorization, in which case, the disclosure will be limited to the PHI specified on the authorization;
    iv. The disclosure is to the Secretary of United States Department of Health and Human Services; or
    v. The disclosure is required by law (See Wellfound Behavioral Health Hospital Policy #800.45).
4. Statement of Purpose Requirement for All Disclosures to which Minimum Necessary Rule Applies
    i. For all disclosures to which this "minimum necessary" requirement applies, when a request is made for access to, or the use or disclosure of, Wellfound Behavioral Health Hospital PHI, Wellfound Behavioral Health Hospital shall determine whether the request includes a statement of purpose. If the request does include a statement of purpose, Wellfound Behavioral Health Hospital shall release only the minimum amount of information necessary to meet the stated purpose of the request. If the request does not include a statement of purpose, Wellfound Behavioral Health Hospital shall contact the requester to obtain the purpose for the request, document the contact with the requester, and take the appropriate action.
5. Routine Disclosures (e.g. Workers' Compensation, Third Party Payors)
    i. Wellfound Behavioral Health Hospital may disclose PHI on a routine, recurring basis to third parties, such as ambulance companies, revenue recovery agencies, or insurance payors (including but not limited to Medicaid, Medicare, private insurers, and workers' compensation insurers or administrative agencies) without authorization, for the purposes of obtaining payment for health care, and to the extent necessary to comply with applicable laws.
    ii. The first time that a Wellfound Behavioral Health Hospital facility or department receives a request for PHI from such an insurance payor or other third party, and each

time that the request is modified thereafter, the facility or department shall review the request to ensure that the type and amount of PHI that is disclosed is limited to what is necessary in order to achieve the third party's purpose.

iii. For guidance on routine disclosures, please contact the Privacy Officer.

6. Non-Routine Disclosures
   i. Non-routine disclosures and requests (e.g. to law enforcement or to a judicial body) will be limited to only the minimum amount of PHI necessary to accomplish the purpose of the disclosure or request. Non-routine disclosures and requests will be reviewed by the Facility on an individual basis and limited accordingly. Questions regarding the minimum necessary standard requirements should be directed to the facility Privacy Officer and to the Legal Department where appropriate.
7. Requests from Wellfound Behavioral Health Hospital to Other Entities
   i. Wellfound Behavioral Health Hospital also must limit its requests for PHI held by other entities to the minimum necessary to accomplish the intended purpose of the request.

G. Access Control and Termination Procedures
1. It is the policy of Wellfound Behavioral Health Hospital to have departmental procedures (e.g. Human Resources, Security or Corporate Compliance Officer, and Information Services) to grant, modify and revoke access, permissions and rights to Wellfound Behavioral Health Hospital networks, systems, applications, facilities and physical locations to staff based on their roles and responsibilities.
2. It is the responsibility of Department Directors to make access requests for staff under their supervision. This includes updating or revoking access as staff responsibilities change such that a minimum necessary standard is followed.
3. Additional security controls shall be used for remote access to Wellfound Behavioral Health Hospital network which includes justification for access and Department Manager approval.
4. It is the responsibility of Department Directors to ensure that proper certifications are met which impacts access for the staff under their supervision.
5. Access and Controls:
   i. Only properly authorized individuals within the scope of this policy shall have access to ePHI Systems. Such individuals may not attempt to gain access to any ePHI that they are not properly authorized to access. Wellfound Behavioral Health Hospital trains these individuals on proper and appropriate use of access rights.
      a. Wellfound Behavioral Health Hospital takes reasonable and appropriate steps to ensure the identity of the individual is validated prior to granting access Wellfound Behavioral Health Hospital takes reasonable and appropriate steps to ensure that these individuals who work with or have the ability to access ePHI are properly authorized and/or supervised, as set forth in the Authorization and/or Supervision Procedures section of this policy.
      b. Wellfound Behavioral Health Hospital has a documented process for terminating access to ePHI when employment or contracted services of users ends or when access is no longer appropriate.
6. Authorization and/or Supervision Procedures
   i. Wellfound Behavioral Health Hospital has established reasonable and appropriate measures to ensure that individuals who have the ability to access ePHI or work in areas where ePHI might be accessed are properly authorized and/or supervised.
      a. Only authorized individuals who have a need for specific information in order to fulfill their respective job responsibilities are authorized to access ePHI, ePHI Systems or areas where ePHI might be accessed.
      b. Wellfound Behavioral Health Hospital uses a minimum necessary standard, as reiterated throughout this policy and other policies, as the basis for the type and extent of authorized access to ePHI.
      c. Wellfound Behavioral Health Hospital has established a documented process for granting authorization and supervising access to ePHI, including:

d. Department Directors are authorized to request system access (including remote access) for users.
e. Wellfound Behavioral Health Hospital grants different levels of access to ePHI and to areas where ePHI might be accessed based on workforce members' roles and responsibilities.
f.
g. Logging and tracking authorization of workforce members' access to ePHI and to areas where ePHI might be accessed.
h.
i. Logging and tracking authorization of third parties' access to ePHI and areas where ePHI might be accessed.
j.
k. Workforce members are not allowed access to ePHI or to areas where ePHI might be accessed until proper authorization is granted.
l.
m. Wellfound Behavioral Health Hospital has established a documented process for modifying access to ePHI, including:
n.
o. Department Directors are required to periodically review user rights to access ePHI to ensure rights are appropriate based on workforce members' roles and responsibilities through an established process with (COO) or appropriate application groups. Discrepancies must be reported to the Information Services (IS) Help Desk immediately for remediation.
p. Department Directors are responsible for notifying Human Resources when an individual is terminated or transfers within Wellfound Behavioral Health Hospital. This includes contractors and vendors in addition to other workforce members as defined in the Scope statement.
q. Human Resources are responsible for providing daily and monthly terminated Employee lists in a standard format to the COO, Security, the IS Help Desk, and appropriate application administrators.
r. Medical Staff Services (Credentialing) is responsible for notifying COO, Security, the IS Help Desk, and appropriate application administrators, when a doctor is disassociated. Credentialing must also provide a bi-annual disassociated Doctor List to COO, Security, the IS Help Desk, and appropriate application administrators.
s. All outsourced services providers are responsible for notifying the COO, Security, the IS Help Desk, and appropriate application administrators, when an employee of their company is. Outsourced Service Providers must also provide a bi-annual terminated employee list to COO Security, the IS Help Desk, and appropriate application administrators.
t. Wellfound Behavioral Health Hospital, as appropriate, reviews and revises the authorization of access to ePHI or to areas where ePHI might be accessed.

7. Termination Procedures
   i. Wellfound Behavioral Health Hospital implemented a documented process for terminating access to ePHI when the employment or contracted services of individuals within the scope of this policy ends or access is no longer appropriate.
      a. When such an individual provides notice of his or her intention to end employment at Wellfound Behavioral Health Hospital or the individual is terminated by Wellfound Behavioral Health Hospital, the individual's Department Manager gives prompt notice to the IS Department or such other person designated as responsible for terminating access to ePHI for the departing individual so that access can be terminated when s/he leaves.
      b. Wellfound Behavioral Health Hospital logs, tracks, and maintains receipts and responses to such termination of access notices.

c. Employees and contractors who are terminated, or whose association otherwise ends, are prohibited from retaining, giving away, or removing from Wellfound Behavioral Health Hospital premises any ePHI. At the time of his or her departure, the individual shall provide all ePHI in his or her possession to their Department Manager.
d. At the time of departure, each individual must return supplied equipment and property that contains or allows access to ePHI, and the Department Manager must coordinate with the IS Department to ensure that any access to ePHI Systems held by the individual is disabled and removed, by the time of, or if not feasible, immediately after, the individual's departure. The IS Department and/or Business Unit tracks and logs the return of such equipment and property with the individual's name, date and time equipment and property was returned, and identification of returned items, and shall securely maintain the tracking and logging information. The equipment and property that may contain, or allow or enable the individual to access, ePHI include, but is not limited to:
    1) Portable computers, including laptops and iPads;
    2) Name tags or name identification badges;
    3) Security tokens;
    4) Access Cards;
    5) Building, desk, or office keys;
    6) Backup media (hard drives, CDROMs, DVDs, tapes, etc.) and USB drives;
    7) Cellular telephones; and
    8) Smartphones.

H. Training and Security Reminders
1. The Corporate Compliance Officer will provide training on HIPAA on, at least, an annual basis.
2. The Corporate Compliance Officer also periodically issues security information and awareness reminders to the Wellfound Behavioral Health Hospital workforce and may also distribute posters, in-service education, newsletter items and post information to the Wellfound Behavioral Health Hospital website.

I. Sanctions
1. In compliance with the HIPAA Privacy and Security Rules, violations of this policy will be subject to disciplinary action as outlined in the Human Resources Policy and Procedure Manual and in the Bylaws, Rules and Regulations of the Medical Staff.
2. Document Retention
3. Any documentation generated in compliance with this policy will be retained for a minimum of 6 years from the date of its creation.
4. Questions related to access to, or the use or disclosure of, PHI should be directed to the facility Privacy Officer.

V. References TO Regulations and/or Other Related Policies:

Health Insurance Portability and Accountability Act, 45 CFR Parts 160 and 164
Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009)