Title: Privacy & Security Guidelines for Information	
Policy Area: Health Information Management	Owner: Chris Rakunas, COO/CFO
Date of Approval: Approval By:	10/19 Matt Crockett, CEO
Original Date: Revision Dates: Reviewed with no Changes Dates:	10/19 X/XX; X/XX X/XX; X/XX
Signature:	

I. Title: Privacy & Security Guidelines for Information

II. Purpose

To protect the privacy and security of patient information and assure that disclosure of information is in compliance with all federal and state laws governing confidentiality.

III. Policy

It is the policy of Wellfound Behavioral Health Hospital (WBHH) to protect the privacy and security of patient information and to assure that the disclosure of all such information, whether written, verbal or electronic (including faxes), is conducted in compliance with all federal and state laws governing confidentiality. All staff members, medical staff, students, interns, volunteers or other individuals having access to patient information have a responsibility to protect and preserve confidentiality at all times.

IV. Procedure

A. All individuals involved in the collection, handling and dissemination of patient information should be specifically informed of their responsibility to protect patient data and the penalty for violation of confidentiality. This policy will be made known to all employees upon new hire; each employee should indicate an understanding of this policy through a signed statement of confidentiality at the time of employment and retained in the employee's personnel file. This responsibility will not cease with the termination of employment. A breach of privacy and/or security may result in disciplinary action up to and including termination. In addition, students, interns and other non-employed individuals providing services within the hospital should be educated about confidential laws and sign a statement of confidentiality.

B. All patient information is considered confidential and may not be released to anyone without prior written consent from the patient or legal representative or pursuant to a valid court order. Patient information is defined as any written, electronic or verbal information about a current or former patient that is personal and private in nature, including his or her existence in treatment including whether he or she is, or ever was an inpatient or outpatient.

C. All staff will receive inquiries, verbal or written in a professional and courteous manner so that the person making the inquiry understands that hospital staff will address the inquiry within the guidelines provided by law and in the interest and concern of the individual in question. If the inquiry is above the receiving staff member's ability to address, they will refer the inquiry to the appropriate department, person or administration.

D. All visitors entering the hospital (patient families, vendors, maintenance/repairmen, surveyors, sales representatives, a referral source, etc.) should sign a visitor confidentiality sign-in log, acknowledging that they understand that what they see and hear while in the hospital is confidential and should not be shared with others. These forms will be sent to HIM at the end of each month for retention requirements.

E. Patients will not be paged on the overhead paging system, nor should their full

name be posted within the view of other patients or visitors.

F. Patient Confidentiality Code Numbers: In order to protect patient confidentiality, the hospital assigns a confidential code number for each admission. The confidentiality number is the last four digits of the patient's admission number.
    1. On admission, the patient will be informed of his or her code number and his or her responsibility to give it to individuals he or she deems appropriate.
    2. This code will be communicated to the nursing units and the receptionist.
    3. No acknowledgement of patient's current or former presence at the hospital will be given to anyone without the correct code number
    4. Even when the correct code number is given, specific information with regard to the patient's care and treatment cannot be communicated to anyone without the written consent of the patient or individual authorized to give consent, as noted above.

G. Telephone requests for information: Telephone requests for patient information will be carefully screened. Again, patient information can only be released via prior written consent by the patient, except in very limited circumstances.
    1. If staff receives a telephone call regarding a current patient they will ask the caller for a code number and verify in a signed release of information form is completed for that caller prior to providing any verbal information (such as admit date, expected discharge date, condition status, daily and overall). No other information will be provided verbally to the caller.
    2. If the caller has the correct code number for the patient, the receptionist will transfer the call to the appropriate patient line during visiting hours only.
    3. If after visiting hours all calls will be sent to appropriate unit for staff to address.
    4. If the caller does not have the code number, the staff response should be a statement that neither confirms nor denies that patient's presence in the hospital. The staff member should then politely explain the hospital's policy to comply with state and federal laws regarding confidentiality.
    5. Family members, ministers, referring professionals and other healthcare professionals may call to speak with the patient or may attempt to visit. This will be handled as outlined above. Offer to take the caller's name and phone number and if the patient is present in the facility information will be relayed to the patient.
    6. For telephone requests for information on former patients or deceased patients, staff should not provide any patient information. Callers should simply be referred to the Health Information Management department.
    7. For inquiries regarding custodial patients, the same guidelines should be followed but consent should be obtained from the custodian or legal guardian.
    8. Answers to inquiry from law enforcement officials will be handled pursuant to state and federal law. Law enforcement officials will not be permitted on patient units unless accompanied by staff members. If law enforcement officials make an inquiry, take a message or if law enforcement has an arrest or search warrant, make a copy of that document. Notify the HIM/Quality Department, the Chief Executive Officer, the Director of Nursing or designee for direction.

H. Confidentiality of Medical Records:
    1. Patient medical records are confidential documents and are kept for the mutual benefit of the patient, provider, treatment team and hospital in accordance with legal, accrediting and regulatory agency requirements. They are the property of the hospital and it is the hospital's responsibility as custodian, to safeguard

patient information, the patient record, and its contents against access, loss, defacement, tampering and use by unauthorized individuals.

2. The patient's original medical record must not be removed from the hospital except for under court order (specifying release of the original record) or for external secured storage.
3. Review of the medical record by hospital personnel should be restricted to the staff requiring information from the medical record in order to carry out hospital duties.
4. Discharge medical records will be maintained in the Health Information (HIM) department and will not be removed to other parts of the hospital, except as is necessary in the transaction of hospital business. When a record is removed from the HIM department, the record should be signed out by the party removing the record from the department and assume responsibility.
5. No medical record information that is obtained from another hospital, healthcare provider or treatment facility is to be re- released for any reason by any member of WBHH.
6. To insure consistency, request for patient information such as verbal or written inquiries from attorneys, insurance agencies or other persons requesting copies of the records will be referred to the HIM department for processing.

I. Data Collection: The types and amount of information gathered and recorded about a patient should be limited to that information needed for patient care (this might include assessments, psychological testing, satisfaction survey's etc.)
    1. Supplemental data, which is not required for patient care, but desirable for research, education, explanation of the purpose for which the information is requested. The request of information for research must be pre-approved by the hospital's Medical Executive Committee.
    2. The collection of any data relative to a patient whether by interview, review of documents or other, should be conducted in a setting, which provides maximum privacy and prevents release to unauthorized individuals. Staff should refrain from discussing patient related issues in public areas of the hospital (such as the hallway, cafeteria etc.).

J. Security of and Access to Patient Information: All facility staff, medical staff and authorized affiliates (students, volunteers, interns, etc.) are responsible for safeguarding the patient record and its content against loss, defacement, tampering and from unauthorized access.
    1. The patient's medical record will be available only to individuals directly involved in his or her treatment for the monitoring of its quality and by other individuals only on his or her written authorization or that of his or her legal representative.
    2. All closed medical records will be housed in a physically secure area under the immediate control of the HIM manager.
    3. All open medical records will be maintained on the nursing units or outpatient areas that are accessed only by authorized personnel. Open records are not allowed to be removed from these areas. Medical records will not be left in unattended areas accessible to unauthorized individuals.
    4. Financial records, correspondence, hospital bills, insurance information or other individually identifiable patient information maintained by the hospital are subject to this policy for maintenance of confidentiality.
    5. Medical records and other patient data records/files should be retained according legal, accrediting or regulatory agency requirements, then stored or disposed of according to the approved retention schedule and hospital policy.
    6. All patient information that is disposed of in accordance with the retention policy will be shredded in the approved method.
    7. There are very limited conditions under which original medical records may

be removed from the premises. It may be required as a response to a properly executed court order or for remote storage. Off premises storage areas are locked and secured to prevent access by unauthorized persons.

8. In the event that a medical record requires extraordinary means of security, (critical incident, legal action, etc.,) the medical record will be stored in a sequestered file. Only records considered extremely sensitive or those involved in legal proceedings will be stored in this manner.

K. Situations when consent may not be required**:** There are limited situations for which the patient's consent my not be required in order to release information These may include:
   1. Review by accrediting or licensing agencies
   2. Valid court order from a court in Washington
   3. Hospital reports of abuse or neglect to government agencies/law enforcement
   4. Duty to Warn or Protect
   5. An emergency in which a life-threatening situation exists, and consent is unobtainable from the patient or next of kin. In emergency situations, medical information may be released to medical personnel without the individual's consent. In this case, record the following information in the medical record:
      i. The date the information was released and method (i.e. phone, fax, etc.)
      ii. What information was released
      iii. The person (first, and last name) and facility to whom the information was released
      iv. The nature of the life-threatening situation and the reason the consent could not be obtained, and
      v. The name of the person releasing the information

L. Cameras/Tape recorders/video recorders: No outside cameras, tape recorders, video recorders or cell phone recordings will be allowed inside the hospital without authorization from administration. No photographs, voice or video recordings may be made without prior written consent from the patient.

M. Computerized information: Computerized patient information is equally as confidential as information collected through a manual system and as such, the same policies and procedures apply. The liability for unauthorized disclosure is the same. Passwords and controlled access to computer applications will be established to prevent unauthorized persons from accessing confidential information.

N. Inquiries from the media (newspapers, television, etc.) will be referred to the Chief Executive Officer or designee.

O. When a question of appropriateness and/or legality arises that is not covered by a specific procedure in regard to confidentiality, contact your supervisor, HIM department or Director of Quality Management.