University of Kentucky / UK HealthCare Policy and Procedure	Policy # A06-100
Title/Description Privacy Investigations & Breach Notification	
Purpose: This policy identifies the process for: 1. Investigating alleged or suspected violations of patient privacy at UK HealthCare facilities in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and implementing regulations, and 2. Determining whether a breach of a unsecured protected health information (PHI) has occurred and if so notifying the patient, the Secretary of the U.S. Department of Health and Human Services (HHS) and, when necessary, the media in accordance with the Health Information Technology for Economic and Clinical Health (HITECH), part of the American Recovery and Reinvestment Act of 2009 (ARRA), and implementing regulations.	

Policy

Suspected or alleged inappropriate acquisition, access, use or disclosure of a patient's PHI shall be reported immediately to the UK HealthCare Chief Privacy Officer for investigation. The Chief Privacy Officer may be reached by calling (**859)323-1184** or **(859)323-8002** or the compliance hotline 877-898- 6072.

The UK HealthCare Chief Privacy Officer or his or her designee shall:

1. Investigate and respond to inquiries and complaints made through the Compliance Hotline, telephone calls, e-mail, written notice, in person, referral from management, customer service, or through other means;
2. Investigate and monitor compliance with government regulations and internal policies that relate to a patient(s)'s privacy;
3. Recommend corrective action and system improvements in areas that present HIPAA privacy compliance risks; and
4. Conduct the breach notification analysis during the investigation phase to determine whether a breach of unsecured protected health information has occurred and if so, notify the affected patient or representative(s); the Secretary of the U.S. Health and Human Services (HHS) and, for a breach affecting 500 or more patients, the media. Inform the privacy officer at the Lexington Veterans Affairs Medical Center (VA) if the suspected breach involves a patient seen at that facility.

Definitions

Breach

Breach is defined as the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted by the Privacy Rule which compromises the security or privacy of the PHI unless, as determined by the UK HealthCare Privacy Officer or designee, it is excluded from the definition of breach in the Breach Notification Rule or there is a low probability that the PHI has been compromised based on the risk assessment conducted in accordance with this policy.

Breach Notification rule

The Breach Notification Rule is the regulatory provisions and requirements for notification in cases of a breach of unsecured PHI under HIPAA.

Enforcement Rule

The Enforcement Rule is the regulatory provisions for compliance and enforcement of HIPAA.

Privacy Rule

The Privacy Rule is the regulatory requirements for protecting patient privacy under HIPAA.

Unsecured Protected Health Information

Unsecure PHI is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary.

UK HealthCare Personnel

UK HealthCare personnel is defined for purposes of this policy as any faculty, employee, volunteer, observer, student, vendor/contractor, trainee, or other person whose conduct in the performance of their work for UK HealthCare is under the direct control of UK HealthCare whether or not they are paid by UK HealthCare.

Procedure

Investigation

The UK HealthCare chief privacy officer or his or her designee shall conduct the investigation according to the following phases:

1. Inquiry phase – Fact finding to determine whether there is cause to investigate. Management or supervisor is notified of the interviews and outcomes.
2. Audit phase – Access to records are examined to identify potential inappropriate access, use, or disclosure.
3. Interview phase – Complainant and suspected violators are interviewed if warranted.
   (a) The Chief Privacy Officer or his or her designee and a Human Resources representative or other appropriate University official shall conduct the interviews. In some cases, management or supervisor may also be present during the interviews. Human Resources is notified and updated throughout the process.
   (b) Human Resources and management, supervisor, or other appropriate University official shall consult with the privacy officer on the outcomes and recommend sanctions if necessary. The supervisor is responsible for imposing any sanctions.
4. Breach notification analysis phase- The privacy officer or designee shall make the following determinations when deciding whether a breach has occurred and requires notice:
   (a) Whether an impermissible acquisition, access, use, or disclosure of PHI has occurred.
   (b) Whether the PHI was unsecured.
   (c) Whether the impermissible acquisition, access, use, or disclosure of PHI violates the Privacy Rule.
   (d) Whether there is low probability that impermissible acquisition, access, use, or disclosure compromises the privacy or security of PHI based on a risk assessment of the factors listed in the Breach Notification Rule. This assessment shall only be conducted by the UK HealthCare Chief Privacy Officer or his or her designee.
   (e) Whether the impermissible acquisition, access, use, or disclosure of PHI meets the criteria for exclusion under the Breach Notification Rule.

Note: A privacy complaint is also considered a patient grievance when the patient or the patient's representative makes a written or verbal complaint that is not resolved at the time of the complaint by staff present. The Chief Privacy Officer or designee shall coordinate the response

with the Office of Patient Experience if warranted. See A01-025 Patient Complaints and Grievances.

Notification Procedure

For all breaches of unsecured PHI, UK HealthCare shall notify affected patients or patient representative(s) and the Secretary of the HHS in a manner specified by the HHS. For a breach of unsecured PHI affecting 500 or more patients, the media is notified. All notifications shall be given to the affected patient(s) without unreasonable delay, but no later than 60 days after discovery. A breach is considered discovered on the first day the breach is known, or by the exercise of reasonable diligence would have been known, to UK HealthCare.

The required notification shall be provided by UK HealthCare or its business associate at UK HealthCare's direction and oversight.

To Patient(s) and the Secretary

UK HealthCare shall notify the affected patient(s) and/or their representative(s) via first-class mail at the last-known address or, if the patient or representative has agreed to receive electronic notice and that agreement has not been withdrawn, via e-mail. In addition to such notification, notice may also be provided to the affected patient or representative by telephone or other means, as appropriate, in cases requiring urgency because of possible imminent misuse of unsecured PHI.

For patients who are deceased, UK HealthCare shall provide the notification to the next of kin or personal representative.

If UK HealthCare is required to provide notice to an affected patient and representative for whom it does not have sufficient contact information, UK HealthCare shall provide substitute notice.

When there are fewer than ten (10) such patient(s) and representative(s), substitute notice may be given through an alternative form of written notice, by telephone, or other means.

For ten (10) or more such patient(s) and representative(s), substitute notice shall be in the form of a posting on the UK HealthCare website or in major print or broadcast media in the area where the affected patient(s) and representative(s) are likely to reside. Postings shall be "conspicuous" and posted for ninety (90) days and include a toll-free phone number that remains active for at least ninety (90) days.

UK HealthCare shall not provide substitute notice to the next of kin or personal representatives of deceased patient(s).

Notifying the Media

For breaches of unsecured PHI involving more than 500 residents of a state or jurisdiction:

1. The UK HealthCare Chief Privacy Officer in conjunction with the UK Marketing & Communications Department shall also notify prominent media outlets such as the local newspaper and local TV stations.
2. UK HealthCare shall also notify the Secretary in the manner and form required by HHS.

For breaches of unsecured PHI affecting less than 500 patients:

1. UK HealthCare shall maintain a log of each breach and submit the log to HHS on an annual basis.
2. The log shall be submitted to HHS by March 1st of each year for breaches occurring during the previous calendar year.

Content of Notice

The notice shall contain at least the following elements, in plain language:

1. A brief description of what happened, including the date of breach and the date of discovery of the breach, if known;
2. A description of the types of unsecured PHI involved in the breach (such as full or partial name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information involved);
3. Any steps that patient(s) should take to protect themselves from potential harm resulting from the breach;
4. A brief description of what UK HealthCare is doing to investigate the breach, to mitigate the harm to patient(s), and to protect against any further breaches; and
5. Contact procedures to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, web site, or postal address.

The above information may be given in separate notices, if necessary.

Training

UK HealthCare personnel shall receive training on this policy on a regular basis.

Enforcement and Sanctions

UK HealthCare shall comply with the Enforcement Rule effective September 22, 2009.

UK HealthCare personnel shall be subject to corrective action for violating this policy, including, without limitation, acquiring, accessing, using or disclosing PHI in violation of the Privacy Rule. Any corrective action taken shall be in accordance with University personnel policies (see UK Human Resources Policies and Procedures 62.0).

Documentation

All documentation generated under this policy, including, without limitation, documentation of the investigation, breach analysis, risk assessment and notification, shall be maintained for six (6) years.

Persons and Sites Affected

Enterprise ☒	Chandler ☐	Good Samaritan ☐	KCH ☐	Ambulatory ☐

Departments: [UKHC Policy Sites Departments]

Policies Replaced

☐ Chandler HP ☐ Good Samaritan ☐ Kentucky Children's CH
☐ Ambulatory KC ☐ Other

Effective Date: 9/21/2020	**Review/Revision Dates**: 8/2010; 9/23/2013; 5/9/2017; 9/21/2020

Approval by and date:

Signature _____ Date_____
Name Richard Chapman, Chief Privacy Officer, Review Team Leader

Signature _____ Date_____
Name M. Gwen Moreland, Chief Nurse Executive

Signature _____ Date_____
Name Angela Lang, Chief Experience & Operations Officer

Signature _____ Date_____
Name Jennifer Rose, Chief Administrative Officer

Signature _____ Date_____
Name Jay Grider, MD, Chief Physician Executive

Signature _____ Date_____
Name Colleen Swartz, Vice President for Hospital Operations

Signature _____ Date_____
Name Mark Newman, MD, Executive Vice President for Health Affairs