# Clinical Researcher
# March 2018
# HOME STUDY TEST
# *The Privacy Prism*

## Earn 2.0 Continuing Education Credits

Two articles from the online March 2018 issue of *Clinical Researcher* (see **https://www.acrpnet.org/resources/clinical-researcher/**) have been selected as the basis for a Home Study test that contains 20 questions. For your convenience, the selected articles and test questions are combined and posted in the form of this printable PDF at **https://www.acrpnet.org/professional-development/training/home-study/**, where the test may be purchased. *The test will be active until March 31, 2019.* This activity is anticipated to take two hours. **Answers must be submitted using the electronic answer form online (members $30; non-members $50).** Those who answer 80% or more of the questions correctly will receive an electronic statement of credit by e-mail within 24 hours. Those who do not pass can retake the test for no additional fee.

## CONTINUING EDUCATION INFORMATION

The Association of Clinical Research Professionals (ACRP) is an approved provider of nursing and clinical research continuing education credits.

### Contact Hours

The Association of Clinical Research Professionals (ACRP) provides 2.0 contact hours for the completion of this educational activity. These contact hours can be used to meet the maintenance requirements for certification programs of the Academy of Clinical Research Professionals. (ACRP-2018-HMS-003)

### Continuing Nursing Education

The California Board of Registered Nursing (Provider Number 11147) approves the Association of Clinical Research Professionals (ACRP) as a provider of continuing nursing education. This activity provides 2.0 nursing education credits. (Program Number 11147-2018-HMS-003)

## ACRP DISCLOSURE STATEMENT

The Association of Clinical Research Professionals (ACRP) requires everyone who is in a position to control the planning of content of an education activity to disclose all relevant financial relationships with any commercial interest. Financial relationships in any amount, occurring within the past 12 months of the activity, including financial relationships of a spouse or life partner, that could create a conflict of interest are requested for disclosure. The intent of this policy is not to prevent individuals with relevant financial relationships from participating; it is intended that such relationships be identified openly so that the audience may form their own judgments about the presentation and the presence of commercial bias with full disclosure of the facts. It remains for the audience to determine whether an individual's outside interests may reflect a possible bias in either the exposition or the conclusions presented.

Clinical Researcher—March 2018 (Volume 32, Issue 3)

PEER REVIEWED

# Privacy and Information Security Issues in Clinical Research

Marti Arvin, JD

[DOI: 10.14524/CR-18-0001]

Organizations engaged in clinical research have a number of complex regulations to follow to ensure compliance, with one particularly challenging area of regulations being privacy and information security. Key to understanding the implications of privacy and information security in research is knowing that concerns can arise in each phase of the research project. What happens during one phase of the project can have implications in later phases.

Breaking down the phases and discussing those implications will help clinical research professionals meet regulatory and contractual obligations. As a result, it will also reduce the risks to the organization conducting the research.

There are also multiple laws and regulations that can impact privacy and information security considerations in a research project, including the Health Insurance Portability and Accountability Act (HIPAA),{1} on which this article will primarily focus.

## Phases of the Research Study

For purposes of this article, the phases of a research project will be broken down into the following:

1. Protocol development
2. Grant submission or contracting with sponsors
3. Institutional review board (IRB) submission
4. Conducting the study

5. Closing out the study
6. Ongoing storage of data and data destruction

## Protocol Development

When developing a project, researchers must consider details like: What data do they need? What are the inclusion exclusion criteria? How and with whom will any collected data be shared? From where or whom will data be acquired? Will the data being collected be identifiable or de-identified? As the protocol is developed, each of these questions should be considered not only to explore the hypothesis, but also for the privacy and security implications.

When considering what data are needed, researchers must fully explore the hypothesis to determine what data elements might be included in the protocol. They must identify not only the primary types of clinical data (e.g., historical and physical records, laboratory results, operative reports, etc.), but what other data are necessary. Will the project be collating information from multiple sources? If so, what unique identifier(s) is needed to identify the subject's data across those multiple sources? Further, if the research requires demographic data, that should be identified in the protocol and not merely assumed.

Establishing a protocol that appropriately identifies the right data for the study can have implications later in the study. For example, if the data being sought for review are not clearly articulated in the protocol when a researcher seeks approval for a waiver application under HIPAA, the IRB or privacy board may not authorize the application.

The approving body for the HIPAA waiver application must determine the necessity of the information being requested for the project.{2} If the application lists more data elements than are delineated in the protocol, it could result in questions of why the researcher needs the additional information.

It's also important to use consistent language to discuss how data will be collected, stored, retained, or destroyed. The language must be consistent across all study documents, starting with the protocol. Language that is in the protocol but not carried forward in all other documents can create confusion. It could also result in violations of regulatory obligations or contractual agreements. This lack of consistency across study documents will be discussed more in the sections ahead.

## Grant Submission or Contracting with Sponsors

When research professionals complete documentation for grant proposals, they should follow the grantors' requirements. Those requirements may contain language regarding the need to meet certain regulatory obligations. For example, it is becoming more common for federal regulators to require some level of compliance with the Federal Information Security Management Act (FISMA),{3} meaning the individual completing the grant proposal must understand the varied obligations of compliance under FISMA. If the individual indicates his/her organization can and will meet the FISMA obligations, this involves taking on compliance risks.

Cost implications are another consideration; if a grant is awarded, the additional financial implications of agreeing to certain regulatory compliance obligations must be considered. If an organization accepts funding but is not meeting the obligations, it could result in a False Claims Act{4} violation when the grant comes from a federal agency.

There can also be issues with sponsor contracts under the clinical trial agreement (CTA). If the office negotiating these agreements is not aware of the consequences of the agreed-upon terms, the study and the study team can be impacted. Sponsors may wish to include language about the informed consent document, the HIPAA authorization, record retention obligations, and use of the data once they are acquired.

If the sponsor proposes an informed consent document outlining how the subject's information is protected or viewed, that language must be consistent with the language ultimately approved by the IRB. If it is not, this needs to be reconciled by communicating during the negotiations or ensuring modifications to the agreement.

The CTA may also have language about records retention that differs from the policies of the organization. This means the potential cost associated with the records retention must be factored into the budget, and there must also be communication with the study team to assure its members understand the retention obligation. This is particularly true if the retention language in the CTA differs from organizational policies that make the retention period longer.

### IRB Submission

Once the protocol is done, and often while the funding is being finalized, the researcher will submit the study to the IRB for approval. The IRB has traditionally been tasked with evaluating studies with the protection of the human subjects as its primary focus.

Not only is the IRB responsible for evaluating the merits of the study in the context of the Common Rule,{5} it is often also the body that approves waivers of authorizations under HIPAA. Some institutions may also choose to approve HIPAA authorizations needed in the study, even though there is no regulatory obligation to do so.

### Issues with HIPAA Waiver Application

To review protected health information (PHI) held by a HIPAA-covered entity without subject permission, the researcher will need to submit a waiver application. This is where it is important for the researcher to understand the difference between HIPAA and the Common Rule. HIPAA is applicable to even look at identifiable data; the Common Rule is applicable when there is a desire to record identifiable data. HIPAA is implicated even for non-human subject research if the researcher needs to see PHI.

When a researcher applies to the IRB or an institution’s privacy board for a waiver of the HIPAA Privacy Rule authorization requirement, at least three things should happen:

- Assure that the data being requested in the waiver application are all of the data that need to be looked at and/or recorded. If the study needs 20 data elements but the application only identifies 15, the researcher cannot legally acquire the remaining five data elements.
- If the data being requested go beyond what the protocol delineates as necessary for the study, the reviewing body (IRB or privacy board) should question the researcher regarding why the additional data are being requested. If the researcher identifies the

additional data as needed for the study, then consideration should be given to modifying the protocol. If it is not justified, the waiver application should be adjusted.

- The reviewing body should assess the provisions in the waiver for how data will be protected. IRB or privacy board members may not wish to assess the adequacy of the security protections for the data; however, the HIPAA rule states approval of a waiver requires the researcher to demonstrate "an adequate plan to protect the identifiers from improper use or disclosure."{6}

  A possible win-win is to have the researcher agree or attest in the application that he/she will follow the organization's information security policies and standards. This allows the approving body to determine if an adequate plan exists, without requiring them to assess specific criteria around data protection. This also allows an auditable standard for any oversight office to test against.

### Issues with HIPAA Authorizations

If the study in question is a clinical trial involving the need to access PHI from an entity covered by HIPAA, the researcher will need valid authorization to get the data. In some organizations, the IRB has elected to review the authorization. With or without an IRB review, there are some key areas to assess in an authorization:

- Does the authorization meet all the criteria identified in the HIPAA Privacy Rule for a valid authorization? If all of the criteria are not included, the authorization is not valid and the data cannot be legally looked at or acquired.
- Has the document captured all of the data elements the researcher may desire access to from the covered entity? For example, if the document does not include access to diagnostic test results but that is necessary for the study, the researcher may not review or obtain such information.
- If the study will include sensitive data requiring explicit permission to access (such as HIV status, behavioral health, or substance abuse data), is that specified in the document? For example, the study inclusion criteria require a negative HIV test; however, if the authorization does not provide an option to obtain explicit permission from the subject, the research team will not be able to access the test results. If the blood draw is performed

and sent to a HIPAA-covered entity for analysis, the analysis could be performed, but the results could not be provided to the study team.

- Is the required expiration date appropriate for the nature of the study? If the authorization has an expiration date of one year from signature, but the study participation is anticipated to be two years with an additional four years of follow-up, this would require a new authorization each year of participation and follow-up.

Many research organizations have produced a template HIPAA authorization document for use in research. These templates help ensure all of the required data elements are included for a valid authorization under the regulations. However, having a template does not ensure compliance because the templates must be customized to each study. The study team is still responsible for ensuring the document is completed to reflect its specific study.

**Conducting the Study**

While the study is ongoing, the research team must assure it is meeting any regulatory or other obligations regarding protecting the privacy and security of the data being collected. The research team should have a clear understanding of what was approved by the IRB, what is included in the HIPAA authorization, and what is in the informed consent. The study documents should be in alignment.

As the research progresses, or members of the team change, there must be good communication regarding privacy and information security requirements. For example, if a new team member is added to the study but the individual has not read the study documents, there may be compliance issues. If the individual begins collecting data from sites that are not covered by the waiver of authorization, the data collected would not be legally obtained.

Failure to obtain an authorization is another possible issue. Research professionals have had the idea of “obtaining informed consent” drilled in to their brains for years, but since the advent of the HIPAA regulations, a valid authorization may also be required. Without the valid authorization, any data about the subject obtained from a HIPAA-covered entity would not be legally obtained.

Researchers may still confuse the intent of the HIPAA authorization and the informed consent. Even if there is language about how data will be used and shared in the informed consent, the document must include all of the required criteria for a valid authorization in order to meet HIPAA compliance.

Organizations must consider proper protocol if a researcher fails to get a valid authorization prior to acquiring data; this will raise HIPAA compliance issues for the research organization and the covered entity. It will possibly implicate compliance with the grant or contract for the study. It could also have implications for study integrity if the data cannot be re-acquired in a compliant manner.

Another common area of concern while conducting the study is informed consent. If the person obtaining informed consent is not clear on what any privacy or information security language in the document really means, there could be a misunderstanding by the subject that sets a higher level of expectation than intended.

### Closing the Study

Privacy and security issues must also be considered when a study is ready to close. The same care must be taken at this stage to assess any regulatory or contracted obligations.

If the researcher indicated he/she will eliminate any identifiers for a retrospective records review once the study findings are published, then someone must assure this is done. If the clinical trial phase of the study is done but there will be ongoing follow-up for a number of years, does the authorization cover this long-term collection of data? This can be an issue if the expiration date of an authorization is three years from the date of signature, for example, but the follow-up data collection is intended for 10 years.

### Records Retention and Destruction

Researchers generally have a primary interest in assessing the data and publishing their findings. Once that is completed, they are ready to move on to the next project. However, the records retention requirements to meet regulatory obligations and/or contractual agreements may go well beyond the date of publication.

The research team needs to be aware of the records retention obligations under any applicable regulations, any contractual agreement, and any institutional policy. Each of these may differ. The obligation to continue to protect the data is usually an institutional policy, but often it is the principal investigator and members of the study team who are actually carrying this out.

Study records can hold a wealth of information, some of which might be quite sensitive. Improper maintenance of data can lead to system vulnerabilities and compromised data privacy and integrity. This could lead to the need to notify subjects if their data are acquired by a third party. It could also lead to breach of contract or the inability to produce the data, should a regulatory body wish to conduct an audit.

## Conclusion

Thinking about data privacy and security from the very beginning of the research project is critical. Failure to consider these issues in the beginning can exacerbate matters as the project proceeds. Much more work may be required by the research team to fix issues at a later date that could have been avoided.

Thinking of privacy and information security at every phase of the study will help minimize any noncompliance, reduce regulatory risk, and help ensure that subjects clearly understand what will happen with their data as result of agreeing to participate in the study.

## References

1. U.S. Department of Health and Human Services. HIPAA for Professionals. https://www.hhs.gov/hipaa/for-professionals/index.html

2. *Code of Federal Regulations*. 45 CFR 164.512(i)(2)(iii). https://www.law.cornell.edu/cfr/text/45/164.512

3. U.S. Department of Homeland Security. Federal Information Security Modernization Act. https://www.dhs.gov/fisma

4. U.S. Department of Justice. False Claims Act. https://www.justice.gov/sites/default/files/civil/legacy/2011/04/22/C-FRAUDS_FCA_Primer.pdf

5. U.S. Department of Health and Human Services. Federal Policy for the Protection of Human Subjects ('Common Rule'). https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html

6. *Code of Federal Regulations*. 45 CFR 164.512(i)(2)(ii). https://www.law.cornell.edu/cfr/text/45/164.512

**Marti Arvin, JD,** (marti.arvin@cynergistek.com) is Vice President of Audit Strategy for CynergisTek.

Clinical Researcher—March 2018 (Volume 32, Issue 3)

PEER REVIEWED

# Providing Restricted Access to an Electronic Medical Record for Research Monitoring

Leslie Bell, MA; Stephanie Gentilin, MA; Susan Sonne, PharmD, BCPP; Toni Mauney, BA; Patrick Flume, MD

[DOI: 10.14524/CR-17-0034]

As hospital systems and healthcare institutions adopt electronic medical records (EMRs), this creates a new challenge in the normal conduct of clinical research. When protected health information (PHI) is stored in an EMR, there is inherent risk that general access to these systems for source verification purposes could allow research monitors to also have access to the PHI of non-study participants.

## Background

The International Council for Harmonization (ICH) Good Clinical Practice (GCP) guidelines stress the necessity of identifying a safe and appropriate means of allowing research monitor access to source documentation contained in EMRs.{1} However, there often remains challenges in mitigating security risks when granting third-party access to such systems.

In addition, the Health Insurance Portability and Accountability Act (HIPAA) of 1996's Privacy Rule minimum necessary standard specifies that PHI should not be disclosed unless necessary to achieve a particular function, and that a covered entity should take steps to prevent unnecessary or inappropriate disclosure of PHI.{2}

As technology evolves and becomes increasingly integrated with clinical research, it is imperative that institutional leaders continuously evaluate their policies and procedures for the safeguarding of PHI, as well as their methods for granting appropriate access to those data.

## Considering the Options

Limited research is available on successful implementation of EMR monitoring solutions, but there are descriptions of a variety of methods attempted by clinical research sites.{3} One approach is to utilize study coordinators' time and resources, having them access the EMR system and navigate through patient records while the monitor reviews by an over-the-shoulder approach. This solution consumes excessive coordinator time that could be utilized for other study-related duties, as well as potentially creates scheduling conflicts, as monitors can only be scheduled when study coordinators have sufficient time to spare.

Another approach is to prohibit monitors from accessing EMRs, and instead compile hard-copy "shadow charts" for each study participant. This method has inherent cost burdens related to production, storage, and destruction, as well as the logistical burden of necessitating that all hard-copy records receive the designation of a certified copy. In addition, many monitors view the shadow chart as an incomplete form of monitoring, as there is no way to verify that the chart is complete and free of intentional or accidental omissions.{2}

## Case Study

At the authors' institution (the Medical University of South Carolina [MUSC]), the Epic system was implemented for EMRs. Access to the EMR system for general users is a rigorous process involving investigation and documentation of private information (e.g., Social Security numbers) in order to acquire the requisite unique login and password.

This methodology was in place for all users, creating a large procedural burden for research staff to obtain access for monitors, as well as potentially violating existing contracts with sponsors (e.g., by introducing incongruent indemnification language). In addition, there are regulatory requirements to have a system in place for proactive restriction of PHI to patients who had consented to study participation, which was not readily provided with this process.

Cognizant of the limitations of available methods, MUSC undertook the development of a means of granting external research monitors access to Epic in a way that allowed view-only, real-time access to study patients' complete medical records, while prospectively limiting them to the charts of patients who had consented to the trial being monitored. Here we describe the methods and outcomes with our "solution" to this problem.

## Methods

We solicited approaches from other institutions where Epic was in use to assess if there was an existing approach to secure, compliant monitoring using pre-existing Epic functionality. However, none of the institutions approached were wholly satisfied with the existing solutions.

The various functionality employed by institutions included Epic's Release to Inspector function, the EpicCare Link workflow, and the Epic InBasket functionality. Limitations to these methods identified by users at the institutions included static data that prevented real-time source verification, the presentation of data in a PDF format that was extensive and lacking a method to navigate the document, as well as an inability to eliminate the risk of institutional providers inadvertently sending non-research patient charts to monitors' in-baskets.

Unsatisfied with existing options, the authors of this paper decided to develop their own method of monitor access by working with an analyst at MUSC on a restricted-access template in Epic that employs a dual method of security. This restricted-access template limits user rights so that they have no authorization to make edits to the chart or the template itself, or to navigate anywhere in the system outside their assigned patient list.

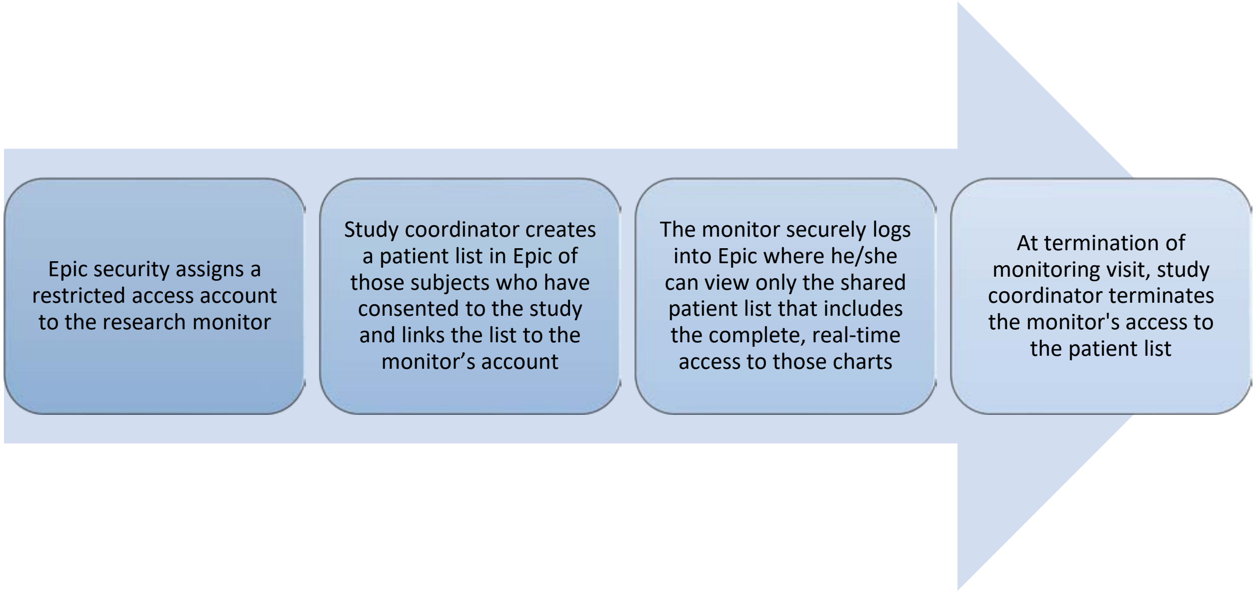
In addition, the restricted-access template removes all visual depictions suggesting the ability to edit or navigate outside the patient chart. Prior to the development of this template, access restriction was not a defined process specific to facilitating monitor access.

An implementation process was developed instructing study teams to notify Epic security requesting restricted access for the monitor prior to the monitor's arrival. A restricted access account is provided that does not allow access into patient records other than those the study coordinator has linked to a monitor's account.

When a monitor logs into Epic, he/she can see only the shared patient list while having access to complete, real-time patient charts. Testing of the template was performed by Epic analysts, university compliance, and Epic clinical and research users. Training of study staff included live presentation (also recorded) and instructional materials. The template was successfully piloted with study teams in January 2015 and broadly implemented in February 2015.

The step-by-step workflow from template assignment to chart access proceeds as follows:

**Figure 1: Restricted Monitor Access Workflow**



Epic security assigns a restricted access account to the research monitor

Study coordinator creates a patient list in Epic of those subjects who have consented to the study and links the list to the monitor’s account

The monitor securely logs into Epic where he/she can view only the shared patient list that includes the complete, real-time access to those charts

At termination of monitoring visit, study coordinator terminates the monitor's access to the patient list

## Results

The restricted-access monitor process was initiated in January 2015 in parallel with the release of the first signed institutional policy outlining the process. The first six months the process was in place was considered a pilot phase under strict oversight by the MUSC compliance office.

During the pilot phase, compliance officers identified no instances of inappropriate access or activity by visiting research monitors. In addition, no negative feedback regarding the new process was received by the university’s Support Center for Clinical & Translational Science

(SUCCESS Center) throughout the pilot phase. Consequently, at the end of six months, the only change made to the process was switching the institutional authority that issued the monitor access accounts from University Human Resources to the Health Information Management team for work flow efficiency purposes. No process or workflow changes were made from the perspective of the research monitor or study team.

As of August 2017, 18 months post-implementation, 490 monitors had utilized the restricted access template. On a monthly basis, up to 100 patient charts have been accessed appropriately, with compliance continuing to come up with zero instances of inappropriate access during post-monitoring visit audits.

## Discussion

The implementation of the restricted-access template in Epic has succeeded in restricting research monitors to consented study patient charts while also allowing them the complete, real-time access required for ensuring human subjects protection and data validation. This has been accomplished in a manner that satisfies security needs at our institution.

Establishing this new institutional process has unveiled the challenge of identifying and incorporating the concerns and requirements of various institutional groups involved in data access across the institution and accommodating all of their requirements. This discovery was the impetus for forming a diverse group of institutional stakeholders who were able to contribute to the development of the monitor access process and corresponding institutional policy.

The group also created a Research Monitor/Sponsor Auditor agreement form—to be signed by both a study team representative and the visiting monitor—outlining the responsibilities of each party. Finally, the group drafted language to embed within contracts between MUSC and corporate research sponsors that spoke to the new policy, to ensure that all sponsors were aware of the necessary requirements for issuing monitors EMR access prior to study initiation.

One limitation identified during this process was the necessity of issuing an MUSC university identity account to research monitors required for them to access Epic. Although these accounts are restricted and secure, almost 500 users had to be added and maintained as account holders in the institutional identity management system. In addition, in order to ensure security, these accounts were prohibited from being utilized remotely, therefore preventing remote monitoring, although such an option was becoming widely requested by corporate sponsors.

In 2017, MUSC upgraded to a newly released version of Epic that contained functionality specifically designed for granting access to research monitors. The solution implemented through this new release was in near exact alignment with our approach, allowing for minimal change in workflow with the adoption of this enhanced functionality. This new approach also eliminates some coordinator burden, allowing the sharing of patient lists with the monitors to be more automated.

The template utilized in this newly released functionality was built using components of Epic's clinical Release to Inspector functionality in combination with the restricted access template that MUSC had designed. This new functionality adds the benefit of allowing for easy remote monitoring; a monitor is sent a link by e-mail that sends him/her directly to an Epic InBox, where view-only, real-time chart information of patients assigned by the study coordinator through the restricted access template may be accessed.

MUSC compliance will test this new functionality and, if approved, new training materials will be developed and the new process piloted by select research teams.

## Conclusion

The development of the restricted-access template and workflow process has been successful in serving its purpose of providing a secure and compliant means of granting monitors appropriate, limited access to the MUSC EMR system prior to the release of this functionality in Epic. This satisfied the security needs of the institution while simultaneously adhering to GCP guidelines and HIPAA privacy rule regulations. The authors hope that the new Epic functionality will allow for the possibility of granting monitors access to patient data remotely in an equally secure manner.

## References

1. U.S. Food and Drug Administration. 1996. Guidance for Industry—E6 Good Clinical Practice: Consolidated Guidance. https://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM073122.pdf

2. U.S. Department of Health and Human Services. 2003. OCR HIPAA Privacy Guidance: Minimum Necessary Requirement. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html

3. Strohmeyer P. 2011. Managing CRA access to electronic medical records. *J Clin Res Best Pract* 7(6). https://firstclinical.com/journal/2011/1106_EHR_Access.pdf

*All authors of this paper are affiliated with the Medical University of South Carolina.*

**Leslie Bell, MA,** (bella@musc.edu) is a Research Navigator with the South Carolina Clinical & Translational Research Institute (SCTR) SUCCESS Center.

**Stephanie Gentilin, MA,** is Director of the SCTR SUCCESS Center.

**Susan Sonne, PharmD, BCPP,** is an Associate Professor of Psychiatry.

**Toni Mauney, BA,** is a Regulatory Coordinator.

**Patrick Flume, MD,** is a Professor of Medicine and Pediatrics.

**MARCH 2018 CLINICAL RESEARCHER**

**HOME STUDY**

# THE PRIVACY PRISM

## Privacy and Information Security Issues in Clinical Research

LEARNING OBJECTIVE

After reading this article, participants will understand the requirements for HIPAA and HIPAA authorization in maintaining privacy of subject information.

DISCLOSURE

Marti Arvin, JD: *Employee of CynergisTek, Inc.*

**1. While there are multiple laws and regulations that impact privacy and information security in a project, which one did the article focus on?**

a) The Common Rule
b) HIPAA (KEY)
c) FISMA
d) PHI

**2. According to the article, how many phases is the project broken down into?**

a) 4
b) 3
c) 6
d) 2

**3. What are the consequences if language in the protocol is not carried forward to all other documents?**

a) IRB approval will not be obtained for the study.
b) The processes across the study will not be aligned.
c) Researchers will not be allowed to collect all data elements as indicated in the application.
d) It could result in violations of regulatory obligations or contractual agreements.

**4. What does it mean if an individual indicates that his/her organization can meet FISMA obligations?**

a) The organization is taking on compliance risks.
b) The organization agrees to all HIPAA-covered entities.
c) It could result in a False Claims Act violation if funding is from a federal agency.
d) Stakeholders had to identify research services required at the institutional level.

**5. What is the primary focus of the IRB?**

a) To approve waivers of authorization under HIPAA.

b) Evaluating studies to ensure protection of human subjects.
c) To evaluate the merits of the study in the context of the Common Rule.
d) To ensure that all the required elements are included in the informed consent form prior to approving it.

**6. What is the difference between HIPAA and the Common Rule?**
a) HIPAA deals with subject privacy and the Common Rule deals with subject safety.
b) HIPAA applies to non-human research only and the Common Rule applies to research in humans only.
c) The Common Rule applies to reviewing results of diagnostic tests whereas HIPAA applies to reviewing protected health information.
d) HIPAA applies to looking at identifiable data whereas the Common Rule applies to recording identifiable data.

**7. According to the HIPAA rule, what is required for an approval of a waiver?**
a) The researcher has to demonstrate an adequate plan is in place to protect the identifiers from improper use or disclosure.
b) The researcher has to highlight in the application all sensitive information that requires explicit permission to access, such as HIV status.
c) The researcher should clearly indicate all the data elements collected are in accordance with regulations.
d) The researcher has to ensure that informed consent and IRB documents are in alignment.

**8. When does a researcher need valid HIPAA authorization to collect data?**
a) If the study involves genomic testing with a separate consent form.
b) If it is a clinical trial involving the need to access PHI from an entity covered by HIPAA.
c) If the researcher is unsure about data elements to be collected and feels it is better to be covered for all aspects of the study.
d) When a researcher needs to contact other physicians to obtain prior diagnostic tests results for subjects that are in the study.

**9. Without a valid HIPAA authorization:**
a) There will be miscommunication regarding privacy requirements.
b) Site staff may not clearly understand what information needs to be collected from the subjects.
c) Any data collected about the subject from a HIPAA covered-entity would not be legally obtained.
d) It will raise compliance issues for the organization and will affect the integrity of the data as well as the grant or contract for the study.

**10. How does considering privacy and information security at every phase of the study assist the project?**
a) It allows for proper follow-up after completion of the study.
b) It ensures that errors are not carried through from one phase of the study to the next phase.
c) It minimizes noncompliance, reduces regulatory risk, and ensures subjects understand what will happen with their data.
d) It creates awareness regarding privacy and information security requirements, assists site staff in understanding what is being collected, and meets regulatory obligations.

## Providing Restricted Access to an Electronic Medical Record for Research Monitoring

LEARNING OBJECTIVE

After reading this article, participants will be aware of the Epic system and ways to grant monitors access to electronic medical records.

DISCLOSURE

Leslie Bell, MA; Stephanie Gentilin, MA; Susan Sonne, PharmD, BCPP; Toni Mauney, BA; Patrick Flume, MD: *Nothing to disclose*

**11. What does ICH-GCP emphasize about access to source documentation contained in electronic medical records (EMRs)?**

a) Electronic systems must be validated to ensure subject privacy and confidentiality.

b) Protected health information should not be disclosed unless necessary to achieve a particular function.

c) Institutions should continuously evaluate their policies and methods for granting appropriate access to EMRs.

d) The necessity of identifying a safe and appropriate means of allowing monitors access to source contained in EMRs.

**12. What impact did compiling hard copies of EMRs have?**

a) Storage space had to be increased.

b) Added the logistical burden of ensuring that all hard copies are certified.

c) Printing and collating of EMRs consumed excessive coordinator time.

d) Created difficulty in scheduling visits, as monitors could only be scheduled after records were printed and certified.

**13. Which institution implemented the Epic system for monitor access to EMRs?**

a) University of South Carolina

b) George Washington University

c) Medical University of South Carolina

d) Multicare Institute for Research and Innovation

**14. Employing a dual method of security ensured that:**

a) The system could not be infiltrated by malware.

b) Two signatories were required to grant the monitor access to EMRs.

c) Users could not make edits or navigate outside their assigned patient lists.

d) There was compliant monitoring of subjects when using the pre-existing Epic system.

**15. How were staff trained on the Epic system?**

a) Webinars

b) Self-paced e-learning modules

c) Reading and understanding new institution SOPs

d) Live or recorded presentations and instructional materials

**16. When was the template piloted to study teams and when was it broadly implemented?**

a) August 2017 and September 2017
b) January 2015 and February 2015
c) January 2016 and February 2016
d) December 2014 and January 2015

**17. After 18 months of implementation, how many monitors had utilized the restricted access template?**

a) 490
b) 100
c) 300
d) 500

**18. What did the diverse group of institutional stakeholders create?**

a) A research monitor/sponsor auditor agreement form.
b) Sponsor awareness of requirements for granting monitors access to electronic records.
c) A platform for access to data that can be shared by both the monitor and coordinator.
d) A research monitor/sponsor institution agreement that was signed by all parties involved in the implementation of the new system.

**19. In 2017, the Epic system was upgraded. What was it specifically designed for?**

a) To meet both institution and regulatory requirements.
b) To automate sharing of patient lists with the monitor.
c) Granting access to research monitors.
d) Ensuring minimal change in the workflow.

**20. What other benefit did the new system implemented in 2017 provide?**

a) It enabled online training materials for the study.
b) It satisfied the security needs of the institution.
c) It reduced study coordinator time for entering data.
d) It allowed for remote monitoring with view-only access.