Clinical Researcher™

The Authority in Ethical, Responsible Clinical Research

March 2018

Volume 32, Issue 3

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

EXECUTIVE DIRECTOR'S MESSAGE

Transforming Energy into Action

Jim Kremidas

[DOI: 10.14524/CR-18-4019]

To say clinical research is an industry whose time for change has come would be a vast understatement. From privacy regulations to informed consent parameters, from the professionalization of the workforce to the adoption of skills-based competencies, we're surfing a wave of change the likes of which we haven't seen before.

As with most periods of evolution, living through it is simultaneously exciting and intimidating. We have an opportunity to harness these forces of change and use them to transform the clinical trial landscape. On the other hand, we risk becoming the passive victims of change if we allow inertia to block us from taking meaningful action.

For example, do we want to let regulatory bodies promulgate new regulations, or do we want to work together to regulate ourselves?

April Beckons

The opportunities for addressing such challenges proactively add to the reasons I'm so excited about how we've redefined our ACRP 2018 annual meeting in April to help drive the professionalization of our workforce. We've added new tracks and new sessions designed to bring together, for the first time, representatives from sponsors, contract research organizations (CROs), and sites to network and learn with each other and all the other kinds of members of ACRP who support the critical day-to-day work of running clinical trials.

Additionally, we will have key industry change agents—including TransCelerate, the Clinical Trials Transformation Initiative (CTTI), and the Association of Clinical Research Organizations (ACRO)—participating and sharing innovative new processes and technologies that are beginning to be integrated into clinical research.

Among other new features for this year's meeting, working with Avoca Quality Consortium, we've put together an industry-first Leadership Track—kicked off by the 2018 Quality Congress. It will give attendees the opportunity to gain an unparalleled view of the changing clinical trial landscape and network with management teams from sponsors, CROs, and sites. This full-day program will equip attendees with transformational approaches to improving clinical research quality.

Let's Keep Talking

Communication, across the entire clinical trial workforce spectrum, is the foundation for realizing positive change. At ACRP, we're working to be a place where the entire industry can come together to share ideas, express concerns, and otherwise help improve clinical trials every step of the way. We all share a passion for providing patients with the best and most professional clinical trial experience.

But we must keep in mind the old saying, "When it's all said and done, there's a lot more said than done." Now is the time for us all to come together and transform energy into action.

Join us at ACRP 2018 in April and be part of the solution!

Jim Kremidas (jkremidas@acrpnet.org) is Executive Director of ACRP.

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

MANAGING EDITOR'S MESSAGE

The Privacy Prism: Multiple Angles on the Personal Nature of Clinical Research

Gary W. Cramer

[DOI: 10.14524/CR-18-4017]

"[W]henever a conflict arises between privacy and accountability, people demand the former for themselves and the latter for everybody else."—David Brin, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*

Avid reader and watcher of fiction that I am, I have of course encountered some of the more famous works of a dystopian nature in which the dark side of living under the rule of a government that seeks to keep its populace under constant surveillance is spelled out to grim lengths. Examples that spring to mind are *Nineteen Eighty-Four, Brazil, V for Vendetta,* and *Person of Interest*.

On the non-fiction side, in the book he is quoted from above, futurist David Brin posits some societal benefits from conditions under which information "is mostly open, in which most citizens know most of what is going on, most of the time," and thinks "that it will be good for society if the powers of surveillance are shared with the citizenry…enabling the public to watch the watchers."{1}

Bringing such thinking home to the level of the clinical research enterprise, who among us has not heard the occasional observation from various sources that drug and device development

would often go much better—ultimately to the benefit of both corporate bottom lines and healthcare consumers—if competing firms were willing to share more data with each other? However, it should come as no surprise if clinical trial participants have reservations about the extent to which key details of their personal data and/or specimens can be identified with them by anyone other than those they think really need access to such information.{2}

Contributors to this issue approach the theme of privacy in clinical research from several different angles, including the viewpoints of participants, data managers, site coordinators, and study monitors. It's plain to see from just these prismatic glimpses into what is, after all, a broad and deep topic, that many competing (though not necessarily warring) interests are at stake, and that the potential perils of forgetting that research participants are individuals—not just bundles of de-identified data—are all too real in research settings.

References

1. https://en.wikipedia.org/wiki/The_Transparent_Society
2. McGraw D, Greene SM, Miner CS, Staman KL, Welch MJ, Rubel A. 2015. Privacy and confidentiality in pragmatic clinical trials. *Clin Trials* 12(5):520–9. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4702499/

Gary W. Cramer (gcramer@acrpnet.org) is Managing Editor for ACRP.

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.

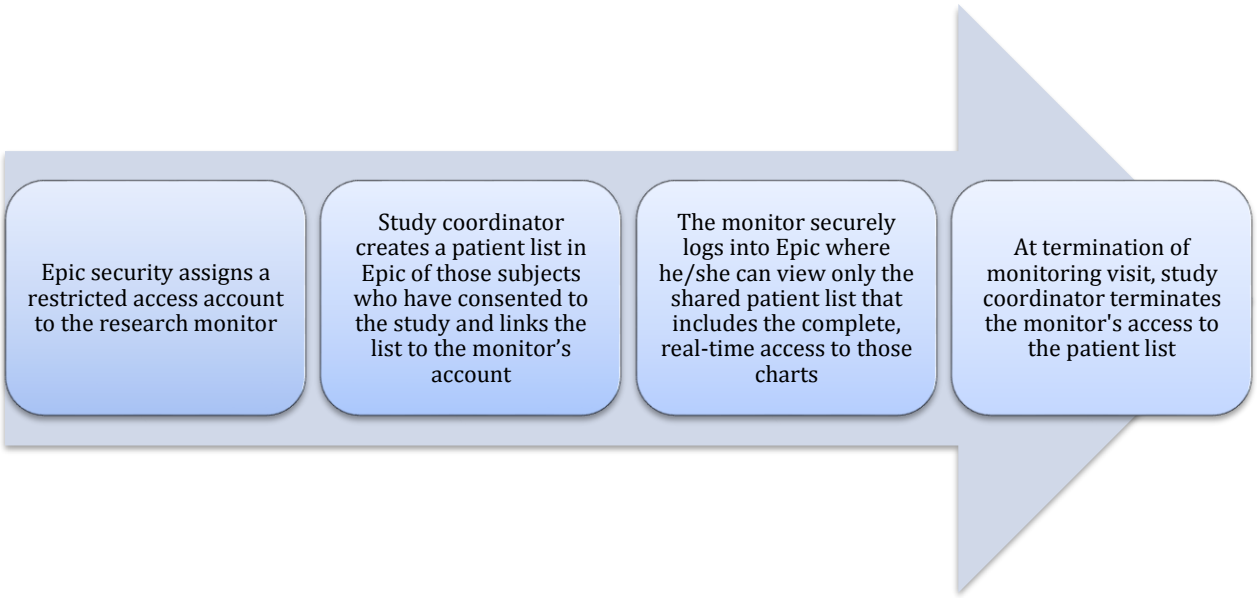
In addition, the restricted-access template removes all visual depictions suggesting the ability to edit or navigate outside the patient chart. Prior to the development of this template, access restriction was not a defined process specific to facilitating monitor access.

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



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.

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

SPECIAL FEATURE

Privacy, Prejudice, and Participation

James Michael Causey; Gary W. Cramer

[DOI: 10.14524/CR-18-4020]

Whether it's via data posted to Facebook, Instagram, or LinkedIn, or shared through e-mails or electronic personal profiles filled out with service providers, clubs, networking venues, or employers, never have so many freely offered up so much information about themselves as they do now through social media and other online platforms.

We can celebrate the birth of a child online, turn others on to a new vacation spot, or share a new culinary discovery while multitasking online at carrying out office duties and job searches, following entertainment sites and hobbies, and purchasing everything under the sun through sites that all want demographic insights into our behaviors as part of the price to pay for access. Others get even more personal, for instance by sharing in-depth details about their health on platforms devoted to patient advocacy for a range of medical conditions and concerns.

Shouldn't we be worried about who can view all (or any) of our personal data, and under what circumstances?

"My U.S. Mail and electronic mail are filled with promises of confidentiality about credit cards, bank accounts, health records, etc.," says Jerry Stein, president and owner of Summer Creek Consulting, LLC, which services clinical trial sponsors and sites. "A fire hose volume of 6-point font agreements flood over me. At the same time, files containing confidential records are continually being invaded by Internet pirates. I have had to freeze my credit records at the three major providers. My experience is not unique."

Yet while Americans, especially those under 30, are increasingly comfortable giving others a window on their world, reported data breaches in healthcare risk giving potential clinical trial subjects pause when considering participating in a trial.

A few recent examples:

- In February, Partners HealthCare revealed its computer network was breached in May 2017, potentially exposing the private information of 2,600 patients.
- Medical Oncology Hematology Consultants was hit by a cyberattack last June. Officials said the hackers targeted certain electronic files on the provider's server and workstations.
- While Augusta University Medical Center officials say less than 1% of patients were impacted by a 2017 breach, it was the second time the organization had been hit with a successful phishing attack within the last year.
- Arkansas Oral Facial Surgery Center was hit by a cyberattack last July that shut the organization out of files, medical images, and details of patient visits. An investigation found that while quickly detected, the virus used in the attack encrypted X-ray images, files, and documents of patients who had visited the provider within three weeks prior to the incident.

While clinical trials weren't impacted in all of these examples, a security black eye for healthcare records of any sort can contribute to the concerns of patients who are considering participating in studies. It's not just that potential participants don't want demographic information and personal identifiers to leak out that may allow others to pretend to be them. Many likely worry as much, if not more, about the ramifications of their medical histories and their personal results from studies being broadcast to anyone with the power to make prejudiced decisions affecting their well-being based on such information, however it was gained.

"I doubt that the clear majority of potential research subjects believe that their personal health information will be adequately protected," says Stein.

It's up to industry to do more to gain patients' trust, experts say. "The process of signing [Health Information Portability and Accountability Act (HIPAA)] and confidentiality agreements within

informed consent forms are *pro forma* exercises [that] may meet international and institutional standards, but there are significant research subject perception issues and enforcement challenges," Stein says.

There's no one-size-fits-all when it comes to protecting sensitive patient health information. However, there are some ways to prevent or mitigate a breach.

"Move quickly to secure your systems and fix vulnerabilities that may have caused the breach," advises the Federal Trade Commission in its "Data Breach Response: A Guide for Business." It suggests the following steps:

- Assemble a team of experts to conduct a comprehensive breach response. Depending on the size of the company, it might include forensics, legal, information security, information technology, operations, human resources, communications, investor relations, and management. Identify a data forensics team. Consult with legal counsel.
- Secure physical areas potentially related to the breach. Lock them and change access codes, if needed. Ask forensics experts and law enforcement when it is reasonable to resume regular operations.
- Stop additional data loss. Take all affected equipment offline immediately. However, don't turn machines off until forensics experts are able to examine them. Never destroy evidence.

If files containing sensitive patient information must be transferred by e-mail, mechanisms to encrypt them and to ensure that password strength is high are necessary. More sophisticated collaboration tools are required to allow file sharing without password sharing.

When sharing files containing anything defined officially in HIPAA as protected health information (PHI) in the context of clinical trials, it is critical to encrypt all PHI. However, such a practice does not provide much protection if the passwords are weak or if the passwords are widely shared. One recent study in healthcare settings indicated that the passwords being used were not strong and could be compromised using a commercial password recovery tool, and that some file-sharing practices used in clinical trials promote the wide sharing of passwords among study staff.

These results suggest that stronger oversight is needed on the transfer of health information in the context of clinical trials, and better training and enforcement (technical and procedural) of good security practices.

Resources for Further Reading

Department of Health and Human Services, Office for Civil Rights. 2003. Summary of the HIPAA Privacy Rule. www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

Fahy D, Nisbet MC. 2013. Debating bioethics openly. *The Scientist* https://www.the-scientist.com/?articles.view/articleNo/36098/title/Debating-Bioethics-Openly/

Institute of Medicine (U.S.) Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule. 2009. *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*. Washington (D.C.): National Academies Press. www.ncbi.nlm.nih.gov/books/NBK9578/

McGraw D, Greene SM, Miner CS, Staman KL, Welch MJ, Rubel A. 2015. Privacy and confidentiality in pragmatic clinical trials. *Clin Trials* 12(5):520–9. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4702499/

Posting 'anonymized' research data may pose threats to patient privacy. 2016. (*Newswise* press release/*Anesthesia & Analgesia*) www.newswise.com/articles/view/653602/?sc=mwhp

Survey: HIPAA Privacy Rule slows scientific discovery and adds cost to research. 2007. (*EurekAlert!* press release/University of Pittsburgh) www.eurekalert.org/pub_releases/2007-11/uops-hpr110807.php

TransCelerate recommends approach for protecting personal data in clinical study reports. 2014. (*PR Newswire* press release/TransCelerate BioPharma Inc.) www.prnewswire.com/news-releases/transcelerate-biopharma-inc-releases-recommended-approach-for-protecting-personal-data-in-clinical-study-reports-273554091.html

James Michael Causey (mcausey@acrpnet.org) is Editor-in-Chief for ACRP.

Gary W. Cramer (gcramer@acrpnet.org) is Managing Editor for ACRP.

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

DEVICE DEVELOPMENTS

Cybersecurity and Medical Devices—A Present-Day Futuristic Dilemma

Eric Distad

[DOI: 10.14524/CR-18-4018]

When I think of cybersecurity, the images that come to mind are nefarious hackers trying to steal personal identification from credit companies, spies breaking into government data repositories as part of an elaborate espionage plot, or even Keanu Reeves plugging into the Matrix to overthrow an out-of-control artificial intelligence. I don't immediately think of medical devices as the next cybersecurity threat. However, the tides are changing, and cybersecurity is something that we in the device industry should get out in front of.

One thing's for sure—computer technology continues to play a critical and growing role in the medical device industry. Trade shows like the Heart Rhythm Society Annual Meeting are full of row upon row of booths displaying devices that range from small, wearable heart monitors to implantable defibrillators—all run and monitored by software that is very likely tied to a network of some kind. Any medical device that is on a network and sends, receives, or stores information can be a target for parties who want that information in bad faith.

Why Disrupt Devices?

Does it seem likely that someone would go through the trouble to hack into an insulin pump to administer someone a lethal dose? Probably not. However, if ransomware can be used to hold someone's credit card information hostage until they pay a "fee" to have it released, how long before the hackers figure out they could probably get a lot more ransom by holding life-saving information or treatment hostage?

While the likelihood of someone hacking into a defibrillator is low, the result of such an action would be serious in the extreme. This is something medical device companies are being forced to consider as they struggle with the high-tech problems that go with their high-tech products.

What Can be Done?

Medical device companies aren't the only ones who have this on their mind; the U.S. Food and Drug Administration (FDA) and the European Union Agency for Network and Information Security (ENISA) has been thinking about it, too. The FDA issued guidance documents for management of cybersecurity in both pre- and post-market settings. The pre-market guidance document, issued in December 2014, recommends a proactive approach in thinking about cybersecurity, and includes a four-point list of cybersecurity information to include in pre-market submissions for applicable devices.{1}

The FDA recommends the inclusion of information on the following considerations:

- Device Description—This should include discussion of each externally facing electronic interface on the devices, its purpose, and indicated use and/or limitations.
- Risk Analysis—Including risks associated with interoperability, potential misuse, and foreseeable combinations of events that could cause potential issues with patients.
- Verification and Validation—Covering details of the verification and validation testing for all device interfaces.
- Labeling—Documentation of the device's intended use for safety and efficacy. The labeling should be compliant with FDA's regulatory requirements on labeling of medical devices.{2}

The post-market guidance document, issued in December 2016, again notes the threat that networked medical devices face and encourages manufacturers to think about how they will approach the issue throughout the product's life cycle.{3} Evaluation of cybersecurity risk for devices is largely dependent on the impact on patients if exploitation occurred, and whether that risk is sufficiently controlled.

The post-market guidance offers recommendations on how to asses this risk based on likelihood of exploit, the impact of exploit on patient safety and device performance, and severity of patient harm if exploited. Guidance is provided for when updates made to protect against potential risks need to be reported, plus the document provides a list of what the FDA considers to be critical components of a robust cybersecurity risk management program. A cybersecurity risk management program should include assessment of the exploitability of the cybersecurity vulnerability, assessment of the severity of patient harm, and evaluation of the risk of potential patient harm.

Conclusion

As medical devices become more technologically advanced and the use of consumer devices to monitor one's health continue to grow, the issue of cybersecurity will continue to be one that developers, contract research organizations, and clinical trial sites are forced to consider and address in order to adhere to FDA guidance and protect patient information and safety. While hacking into a medical device may not seem as appealing to criminals as, say, hacking into the Pentagon, it is the responsibility of device researchers to be prepared if the "bad guys" decide to turn their attention to this sector.

References

1. https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482649.pdf
2. https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM095308.pdf
3. https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf

Eric Distad (eric.distad@syneos.com) is Executive Director for Medical Device and Diagnostics with Syneos Health.

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

DATA-TECH CONNECT

The Downside of Technology

Paula Smailes, RN, MSN, CCRC, CCRP

[DOI: 10.14524/CR-18-4015]

Are you distracted?

I am. Almost all the time. On examination, it seems the biggest reason is that personally and professionally, technology is now too convenient. It's mobile—I take it anywhere and everywhere, and it feels as if I am never escaping it. The work keeps coming and a lot of people expect an immediate response, because it is assumed I have the technology with me at all times to do so.

It goes without question that technology has streamlined many workflows and made our lives better, but what are the downsides to this efficiency and dependence? How about: We do work quicker so we get more work? How about technology addiction? I work in the information technology field, and I am an online instructor in a baccalaureate program. I am professionally required to be wired, but when does it all become too much?

Professional Use

Distraction can be a great thing. In clinical research, we might use distraction with research patients, such as when we are drawing blood from a participant or placing an IV for pharmacokinetics. So, distraction can have a positive connotation. However, when it comes to technology, distraction is on the rise in the workplace with negative consequences.

Problems with distraction at work can lead to inattention to team members, scattered focus and multitasking, lost productivity, and, perhaps worst of all, to patient harm.{1} You may recall that in 2000, the Institute of Medicine came out with *To Err Is Human*, identifying that interruptions

as a likely contributing factor to medical errors.{2} Fast forward to 2013, and it was reported that increasing levels of distraction in healthcare were due to the rise of electronic devices.{3}

Five years later, and the situation has gotten worse. I challenge you to look around during the next work meeting or presentation you go to—how many people are distracted by technology and not paying attention? Are you one of them?

As someone who teaches technology to clinical research professionals, I always make those who attend my classes put their smartphones away before we start. I don't want to see anyone distracted, because the truth is, when they are distracted, I'm suddenly distracted. If I see someone distracted, rather than staying focused on my teaching content, I wonder why the distracted person isn't paying attention? Is something wrong?

To get cooperation with the "tech moratorium," I always promise to break after an hour so my students can take a "technology break" to check in with whatever they may have missed. It's usually successful.

Cognitive Implications of Interruptions

Let's break down what happens when you are interrupted by technology. Your attention from your original task is diverted to the distraction. Once this shift in attention occurs, memory of the primary task begins to decay in order to "make room" for the processes required to deal with the interrupting task, and when the original task is resumed, you may not remember which part of the primary task was last completed.{4}

This can further lead to memory loss of that task, with some variability depending on the intensity of the task, what junction of task completion you were in, and the length of the interruption. The bottom line is that when an individual's attention is shifted away from the original task, the likelihood of an error occurring upon return to the primary task is increased.{4}

Technology Health

To determine your technology health, consider some questions to ask yourself:

- Regardless if the technology use is personal or professional, is our distraction self-inflicted or is it an expectation?
- What is your relationship with technology?
- What boundaries have you set for how technology is impacting your life?
- If your boss sends you a text message or e-mail, what is the expectation for replying? How do you gauge urgency of the message? Is that expectation realistic?
- Are you sacrificing your personal life for a technology relationship? Which is more important?
- Are you constantly looking at or sending e-mail or text messages, be they personal or professional? Are you mainly an instigator or recipient of such communications?

Technology addiction has yet to be classified as an official mental health condition, and is largely used as an umbrella term to describe a variety of obsessive or compulsive online behaviors. What causes someone to develop this addiction isn't very well understood, but job stress and mental illness may contribute.{5}

Having a Healthy Relationship

Some solutions have been identified for mitigating the issue of distraction in the workplace that can be used with respect to intruding technology. These include:

- Establishing a "No Interruption Zone"
- Ensuring a do-not-disturb approach
- Providing staff education
- Determining the best time for necessary interruptions
- Managing mobile devices
- Making system improvements
- Managing alerts, alarms, and noise{6}

Mindfulness of one's behavior and how that impacts or influences others may also be considered. The clinician who is mindful of the negative impact of interruptions and distractions

may react with increased attention, focus, and concentration on his or her work environment.{6}

In professional settings and work environments, challenge yourself to be present in the situation by removing those items that distract you. Consider what message might be sent to a research volunteer who is working with site staff distracted by mobile devices. Or, another consideration might be the distracted study volunteer texting messages and not paying attention to directions. Could that impact study outcomes?

Other interventions that may lead to less distraction include experimenting with short periods of inaccessibility; leaving your smartphone at home one day a week; setting a "not to-do" list, such as not checking e-mail during meetings; practicing tech use in moderation; and making a "tech non-proliferation" pact with a friend.{7}

If you want to limit the number of e-mails you get, don't send them. Rather than hit reply, make a phone call instead. You will likely find that a conversation will settle what would have otherwise been 10 or more e-mails.

Also remember that it's very important to have a work/life balance. Save work e-mails for work hours. Give your family members the attention they deserve when you are home. Personally, I stay very cognizant of my children. I never want them to think my technology relationship is more important than my relationship with them. If I must do computer work at home, I try to do so after they are in bed, so their moments with me are not filled with me staring at my computer or smartphone.

My concluding thought on all this is for everyone to remain cognizant of how your technology relationship is treating you. Perhaps more importantly, how do others perceive your technology relationship? Is your relationship with your smartphone abusive and smothering? If so, maybe it's time to reconsider that relationship.

References

1. DeMers J. 2017. Are you constantly distracted by technology? Here's what to do. *Entrepreneur*. https://www.entrepreneur.com/article/286963
2. Institute of Medicine. 2000. *To Err is Human: Building a Safer Health System.* Washington, D.C.: National Academy Press.
3. Papadakos PJ. 2013. The rise of electronic distraction in health care is addiction to devices contributing. *J Anesthe Clin Res*. https://www.omicsonline.org/the-rise-of-electronic-distraction-in-health-care-is-addiction-to-devices-contributing-2155-6148.1000e112.php?aid=11833
4. Rivera AJ, Karsh B-T. 2010. Interruptions and distractions in healthcare: review and reappraisal. *Qual Saf Health Care*. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3007093/
5. Addiction.com. Technology Addiction 101. https://www.addiction.com/addiction-a-to-z/technology-addiction/technology-addiction-101/
6. Beyea S. 2014. Interruptions and distractions in health care: improved safety with mindfulness. Patient Safety Network (PSNet)/Agency for Healthcare Research and Quality/U.S. Department of Health and Human Services. https://psnet.ahrq.gov/perspectives/perspective/152/interruptions-and-distractions-in-health-care-improved-safety-with-mindfulness
7. Soong J. 2008. When technology addiction takes over your life. *WebMD.* https://www.webmd.com/mental-health/addiction/features/when-technology-addiction-takes-over-your-life#1

Paula Smailes, RN, MSN, CCRC, CCRP, (Paula.Smailes@osumc.edu) is a member of the ACRP Editorial Advisory Board and a senior systems consultant and principal trainer for clinical research at The Ohio State University Wexner Medical Center. She also is a visiting professor with Chamberlain College of Nursing.

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

Introducing ACRP's 2018 Class of Fellows

[DOI: 10.14524/CR-18-4016]

Being named a Fellow of the Association of Clinical Research Professionals (FACRP) is a mark of distinction. Launched in 2017, the ACRP Fellowship program recognizes those who have made substantial contributions to the Association and the industry at large, as evidenced by: ACRP certification/ACRP education, leadership contributions to ACRP, and contributions to the field of clinical research. Fellowship highlights excellence and commitment to ACRP, and is suitable for only a small, select number of clinical research professionals who are lauded as global leaders.

ACRP is proud to announce the 2018 Class of Fellows as the second in what aims to be a long and distinguished line. The new Fellows will be honored at the ACRP/AVOCA Awards and Recognition Ceremony on Friday, April 27, during the ACRP 2018 annual meeting.

Suheila Abdul-Karrim, CCRA, CCRT, MICR CSci, RQAP-GCP, FACRP, is an independent clinical research consultant providing services and training to pharmaceutical industry sponsors, clinical research organizations, clinical investigators, and clinical research associates (CRAs). Based in Johannesburg, South Africa, she has a post-graduate degree in science from the University of Witwatersrand with more than 21 years of clinical trials experience as a CRA, clinical research manager, auditor, and Good Clinical Practice (GCP) trainer. She has maintained her Certified Clinical Research Associate CCRA designation since 2000, and is actively involved with ACRP, previously as an item writer for the Global CRA Certification Exam and currently as Chair of the Professional Development Committee, for which she also serves as the Editorial Advisory Board Liaison. She is also the ACRP South African Chapter Chair and leader of the ACRP GCP & Ethics Interest Group.

Jeri Burr, MS, RN-BC, CCRC, FACRP, is Executive Director of the Trial Innovation Center at the University of Utah. A board-certified Pediatric RN, she is a clinical research management professional with two decades of experience in such areas as training, mentoring, and motivation of clinical research operations teams. She has a Master of Clinical Research Organization and Management degree. She also has broad regulatory experience, including coordinating industry-sponsored and National Institutes of Health–sponsored trials, and managing large investigator-initiated, multicenter clinical trials. Currently, she is a member of the ACRP annual meeting Content Advisory Board and serves on the Board of Directors for the Greater Salt Lake City Chapter of ACRP. As an advocate of improving children's health globally, she served as a volunteer pediatric nurse on the USNS Mercy, a medical mission in the Philippines in 2012, providing pre- and post-operative nursing care to Filipino children. In 2015, she traveled to Africa, deep into the Zimbabwean bush on a medical humanitarian mission. As a Master Trainer for Helping Babies Breathe (HBB) and pediatric nurse volunteer, she taught HBB and provided clinical nursing care at various rural clinics throughout Zimbabwe.

Kelly Cairns, MA, BASc, APMR, CCRA, **FACRP**, is currently the Leader of Clinical Trial Operations and Business Support at Boehringer Ingelheim Canada Ltd, a large multinational pharmaceutical company in Burlington, Ontario, Canada. In this role she leads a team of more than 10 field-based positions, 25 in-house research staff, and three managers. Prior to this position she was the Manager of Investigational Supplies, Senior Research Associate, Research Associate, and Clinical Trial Administrator, all with Boehringer. Including the positions she has held at Boehringer, she has more than 25 years of research experience as a study coordinator, clinical research associate (CRA), and project manager in a vast array of therapeutic areas, including HIV/AIDS, metabolic, CNS, cardiovascular disease, dermatology, immunology, and respiratory. She completed her Master's degree in Leadership Studies in addition to her Bachelor of Applied Science, both from the University of Guelph. She has served in many roles with ACRP, ranging from the Executive Committee of the CRA Forum, ACRP Canadian Chapter member, CRA Certification Exam Committee item writer/member, and Chair of the Global CRA Certification Exam Committee. She is currently serving as Chair of the ACRP Academy Board of Trustees. She has maintained her CCRA certification since 2001.

Stephanie Christopher, MA, FACRP, has dedicated her career to improving communication and developing tools to make clinical trials more efficient and patient-centered. She started her career with an academic public health team, working on interventions to improve the quality of communication between physicians and parents of newborns with abnormal newborn screening results. In 2012–13, she went on leave from her academic position to do a special assignment for the U.S. Food and Drug Administration's Center for Devices and Radiological Health, updating and training staff on a new risk communication process. In addition to her roles in advancing clinical research, she taught principles of effective communication as an adjunct instructor at Marquette University for five years. She has been a Certified Clinical Research Coordinator (CCRC) since 2008 and remains an active member of the Minnesota Chapter of ACRP.

Norbert Clemens, MD, PhD, CPI, FACRP, is a board-certified physiologist. His broad exposure to worldwide healthcare issues includes service in several academic positions; as Medical Director for Intersan GmbH, PAION, and Valeant Pharmaceuticals International; as General Manager and Head of Global Clinical Trial Services at Analytica International GmbH; and as Vice President Clinical Operations at Impulse Dynamics, based in Stuttgart, Germany, his current position. He has been a board member of the research and development section of the German Association of the Pharmaceutical Industry, and has served as President of the German Society of Pharmaceutical Medicine and as Treasurer of the International Federation of Associations of Pharmaceutical Physicians for several years. He is a well-known trainer for investigators and site staff. He has served on the ACRP Board of Trustees as Vice Chair, Chair, and Immediate Past Chair, and is a charter member and Secretary of the German Chapter of ACRP.

Joy L. Frestedt, PhD, CCTI, RAC, FRAPS, FACRP, is President and CEO of Frestedt Incorporated and Alimentix, the Minnesota Diet Research Center. She has managed clinical trials, negotiated regulatory submissions, and updated quality systems for nearly 40 years in healthcare, pharmaceutical, medical device, and food industries, including for the University of Minnesota, Orphan Medical, Johnson and Johnson, AstraZeneca, CNS Therapeutics, Mayo Clinical Trial Services, Medtronic, and many others. She holds a PhD in Pathobiology from the University of Minnesota Medical School and BA in genetics from Knox College. She is among the "100 Most Inspiring People in the Life Sciences Industry" (*PharmaVOICE,* 2011) and top 25

"Industry Leaders" (*Minneapolis/St. Paul Business Journal*, 2011). She recently authored "Warning Letters: 2016 Reference Guide" with Barnett International and "FDA Warning Letters About Food Products: How to Avoid or Respond to Citations" with Elsevier. She has served on the ACRP Editorial Advisory Board and with the Global Exam and Regulatory Affairs Committees.

Michael R. Hamrell, PhD, RAC, FRAPS, RQAP-GCP, FACRP, CCRA, is the President of MORIAH Consultants, a regulatory affairs/clinical research consulting firm located near Los Angeles, Calif. He has worked in drug development, clinical research, compliance, and regulatory affairs for more than 30 years. He has also worked at the National Institutes of Health and as a reviewer in the Center for Drug Evaluation and Research at the U.S. Food and Drug Administration. He spent several years doing basic research, first as a Research Fellow at Duke University and later as an Assistant Professor of Pharmacology at the McGill University Cancer Center. He has a PhD in Pharmacology from the University of Southern California and a BS in Biochemistry from the University of California, Los Angeles. He is a Past Chair of the Editorial Advisory Board and has served on the Training and Development Committee with ACRP.

Joy Jurnack, RN, CCRC, CIP, FACRP, is with Northwell Health at North Shore University Hospital. A former Clinical Nurse Specialist for the Liver Transplant Team, she stumbled into research when introduced to it by a hepatologist. Initially certified as a CCRC in 1997, and recertified in 2003, she participated in clinical research in hepatology HCV/HBV, with the AIDS Clinical Trial Group, HIV/HCV in hemophiliacs, and synthetic hormones for post-menopausal women. She also assisted in opening a Phase I Dermatological Unit and taught Good Clinical Practice to investigators, and now works with chronic kidney disease patients with issues like anemia and high potassium. Through it all, she has maintained her clinical specialty in research on human subjects, and says that, as ACRP grows and contributes to the profession, she plans on being part of the growth and enriching the careers of young or not-so-young clinical research professionals. She serves on the Academy Board of Trustees and is a prior member of the ACRP Ethics Committee.

Anita S. Kablinger MD, CPI, FAAP, FAPA, FACRP, completed her undergraduate work at McMaster University and attended medical school at Rosalind Franklin University of Health

Sciences before engaging in psychiatry residency training. She has conducted more than 160 trials as principal investigator or sub-investigator for industry, academic centers, and the National Institute of Mental Health over the past 20 years in academia. Areas of research and clinical responsibilities have included psychosis, mood disorders, and substance abuse.
She has also been a Psychiatry Program Director for 15 years, mentoring undergraduate students, graduate level residents, and junior faculty in patient care, education, and research. Currently, she is a tenured Professor in the Department of Psychiatry and Behavioral Medicine at the Virginia Tech Carilion School of Medicine in Roanoke, Va. and the Director of the Clinical Trials Research Program. She serves as a member of the Global CPI Exam Committee and the Content Advisory Board for the ACRP annual meeting.

Kathryn L. Kimmel, CCRC, CCRA, ACRP-CP, FACRP, decided to explore opportunities in clinical research after working 15 years in a hospital-based laboratory. In the 22 years she has been in the clinical research field, she has worked as a clinical research coordinator (CRC), a director of a multitherapeutic clinic-based research department, a clinical research associate (CRA) and a regional manager of CRAs. She has also served as Chair for the Phlebotomy exam for NCA, and as a committee member and Chair of the ACRP Global CCRC Exam Committee. She is the current Chair of the Association Board of Trustees (ABoT) for ACRP, and has served as a board member and Chair of the Academy Board of Trustees and as ABoT's liaison to the Academy Board. She has also served at Chair of the ACRP Governance Committee and as a member of the ACRP Nominating Committee. She was a charter member and served as President and Program Chair of the former Inland Northwest Chapter of ACRP. She has maintained her ACRP certifications for both CRC (20 years) and CRA (13 years), and is very passionate about certification and the value it brings to the industry. She is currently a Senior Clinical Research Associate with PRA Health Sciences.

David J. Morin, MD, FACP, CPI, FACRP, has been a principal investigator on hundreds of studies since 1989. He became a Certified Principal Investigator (CPI) in 2007 and Credentialed Clinical Research Trainer (CCRT) for ACRP in 2010. He received the "Outstanding Physician Leadership" award by ACRP/APCR in 2012. He co-developed the "CRC Bootcamp" and serves as a principal instructor for ACRP. He received his pharmacy degree with High Distinction at the University of Rhode Island, his MD with Honors at the University of Vermont, and residency

training at the University of Virginia. He is a board-certified Internal Medicine specialist and is a Fellow of the American College of Physicians (FACP). He joined Holston Medical Group in 2008 as the Director of Research. He is a published author and speaker and has developed investigator-initiated trials. He is on the ACRP Board of Trustees and serves as a member of the Governance Committee.

Robert J. O'Connor, MS, CCRA, FACRP, is currently a Senior Clinical Scientist and Clinical Investigator in the BioSciences Department at The Procter & Gamble Company. He had earlier worked as a clinical research associate (CRA) at Kendle Research Associates in Cincinnati, Ohio, and at ClinTrials in Nashville, Tenn. He joined Procter & Gamble in 1994 and has worked on more than 260 clinical trials, of which he has been the principal investigator on 86. He has also been a full member of the company's internal institutional review board. He has extensive experience in clinical research education and training and has been an adjunct professor in the Clinical Research Certificate Program at the University of Cincinnati since 2008. He has been a member of ACRP since 1992 and is a former item writer for the CCRA Exam, former Chair of the CCRA Exam Committee, and former Chair of the ACRP-CP Exam Committee. He was a founding member of the Greater Cincinnati Chapter of ACRP and currently serves as Chapter President. He has held his CCRA designation since 1996. He received the ACRP Exceptional Contribution to Clinical Research Award at the ACRP 2016 Global Conference.

Matthew D. Paul, MD, CPI, FACRP, is a recognized expert in cataract surgery and listed as a "Top Doctor" in *Connecticut Magazine*, *Castle Connolly Top Doctors*, and *U.S. News & World Report*. A participant in more than 16,000 cataract operations, he also is a Fellow of the American College of Surgeons and the American Academy of Ophthalmology. He has held his Certified Principal Investigator (CPI) designation since 2006 and has chaired the Global CPI Exam Committee for four years. He is a Phi Beta Kappa, Sigma Xi Graduate of Wesleyan University, where he earned High Honors for his Honors Thesis. He attended medical school at Columbia University College of Physicians and Surgeons and graduated with the Behrens Prize in Ophthalmology and the Spotnitz Prize in Oncology. As an intern in Internal Medicine at Beth Israel Hospital, he was recognized as "Best in the Emergency Room" and "PGY1 of the Year." After his time as Chief Resident at the Harkness Eye Institute, he entered private practice in Danbury, Conn. He is President of an ophthalmology-subspecialty group of 14 doctors with

additional offices in New Milford and Prospect, Conn. He entered the research arena in 1992 and has participated in more than 70 Phase I–III studies. He also has mentored more than 15 students who have contributed to more than 20 presentations at major ophthalmic meetings.

Deborah Rosenfelder, CCRC, FACRP, is currently a Clinical Data Scientist for Bard. She is responsible for review of data on a continuous basis and coding of adverse events, as well as coordinating the Clinical Events Committee and Data and Safety Monitoring Board meetings. She has more than 36 years of healthcare industry experience. Therapeutic areas of expertise include critical and coronary care, oncology, cardiology, neurology, and device research. She began her healthcare career as a critical care nurse with 16 years of experience. For more than 15 years, she was a Research Coordinator at a large metropolitan teaching university overseeing drug and device trials. She has lectured on topics related to cardiology device and drug trials, recruitment, risk-based monitoring, and other research-related topics. She has been an active member of ACRP for more than 22 years, and is involved with the Medical Device Interest Group of ACRP as Chair. She also has served on the Editorial Advisory Board and the ACRP Global Conference Planning Committee, and is currently Chair of the Training and Development Committee. In addition, she is a Past President of her local ACRP Chapter.

Christine Senn, PhD, CCRC, CPI, ACRP-CP, FACRP, is Chief Implementation Officer at IACT Health, a multispecialty research management organization with clinical sites throughout the Southeast. She engaged in research in obsessive-compulsive disorder at Concordia University in Montreal, eating disorders at Douglas Hospital in Montreal, and pediatric oncology at the University of Vermont. Since joining IACT Health in 2007, she has worked as a Clinical Research Coordinator, Site Manager, and Chief Operations Officer before moving to her current role. She holds her PhD in Psychology and has Master's degrees in both Clinical Psychology and in Advertising and Public Relations. She is certified by ACRP as a Certified Clinical Research Coordinator (CCRC), a Certified Principal Investigator (CPI), and a Certified Clinical Research Professional (ACRP-CP).