

21 CFR Webinar (Transcript)

[music]

Mary Kay Lofurno: Hi! I'm Mary Kay Lofurno, and I just want to welcome you to the second in a series of webinars on compliance and validation topics, put on by Veracord and its division, 21 CFR Consulting. This series is sponsored by SyberWorks, Inc. Veracord and its division, 21 CFR Consulting, is headquartered in San Jose, California, and serves the FDA Regulated Life Science industry, which includes pharmaceutical, biotechnology, and medical device companies. Veracord offers compliance consulting services nationwide, specializing in validation, IT compliance, clinical, medical, and regulatory affairs. SyberWorks specializes in custom e-learning solutions, and learning management systems in the FDA regulated compliant industries.

My name is Mary Kay Lofurno. I'm the Marketing Director for SyberWorks, and your host today. We're really glad to have you. Today, I'd like to go ahead and introduce our speaker David Park Schutz, Veracord Founder and CEO, currently heads Veracord's global sales, serving Fortune 100 clients in the validation compliance sectors.

Under Mr. Schutz's leadership and vision, Veracord's clients now include leading pharmaceutical, biotechnology, and medical device companies. Veracord remains the premier vendor for three of the top 10 global medical device companies. Park's unwavering business development efforts have strengthened Veracord's signature in the industry, as a company with integrity and uncommon commitment to clients.

After the presentation, we will be having a question and answer session. Please feel free to email us your questions. Park will do his best to answer all of those, but don't worry if we don't get to your question during the question and answer period. We will be sending out an email with a write-up of all the submitted questions and answers in the days following the webinar today. So, without any further delay, I'll turn the conference over to Park.

David Park Schutz: Hello, everybody. Thank you very much for joining our conference today. Again, my name is Park. I'm the President/Founder of Veracord. We're a San Jose, California-based provider of validation and compliance consulting services, and are fortunate enough to have a number of prominent companies as our clients, for whom we are very grateful. The purpose of this presentation is to share Veracord's viewpoints and provide an overview of 21 CFR Part 11, but a bit of emphasis on its applicability.

21 CFR Part 11 affects every life science organization, or LSO, and by that, I mean, pharmaceutical, biotech, or medical device companies, or any combination thereof. As we know, there's biopharmas and there's medpharmas, and etc. There's all kinds of combinations these days. All these, that are governed by the FDA. There are risks and penalties if systems are found to be non-compliant.

I don't want to go over the groans in the audience, because I'm not going to spend too much time on the background, but I did just want to touch on it lightly. The FDA has always been concerned with product that is ingested, digested, or introduced into the cellular structure of any people. Therefore, it stands to reason, that anything involved from the production to the person should fall under control and scrutiny. Especially, these days, the need for these controls and vigilances has never been so great, as with the current issues relating to terrorism, and etc.

Do you guys remember reading the book by Upton Sinclair entitled "The Jungle?" It was an exposé of the Chicago meatpacking industry, and contributed to the rising awareness of the need for regulations for public safety. Well, that book and that whole situation that it exposed was part of what led historically to the formation of the FDA. The significant milestone here is that, after a variety of different issues, we have one of our first predicate rules or sort of

guidances for industry, that was pushed out by the FDA in 1949. That became a foundation of things that we'll see later on.

Here are some of the additional milestones that occurred. Tragically, many of the big milestones that moved the development of the FDA into its present position, unfortunately, were just tragedies. Drugs were put out and they wound up killing people or causing blindness, etc.

With respect to Part 11, in particular, it was originally issued in 1997 in response to requests from the life science industry, which recognized that fully electronic data acquisition, evaluation, management and archiving, could significantly improve workflow. So, it actually wasn't something that was pushed on the industry. It was something that was requested by the industry.

The FDA approval process was expected to be shorter, and access to documentation was likewise expected to be faster and more productive. Regrettably, the first guidance was sufficiently open for interpretation, that the reaction to it was that people wound up going overboard, the companies wound up going overboard. So, there was huge amounts of money being spent, and with lots of accusations, being that the Part 11 guidance was actually slowing down productivity, because of all the requirements for becoming compliant with the rule and some of the FDA warnings and consent decrees, and etc., that followed.

The rewrite of Part 11 was published in September 3rd, 2003, and made some significant adjustments, which included narrowing the scope by defining a limited set of records subject to Part 11, allowing, based on documented risk analysis, less stringent application of Part 11 requirements to validation, audit trail, copies of records, and record retention. Finally, it provided exemptions for some legacy systems or some systems that were operational prior to August 20th, 1997, which was the effective date for Part 11.

So, narrowing the interpretation of scope is probably the most significant aspect of the Part 11 final guidance. Verbiage changes between the draft and final versions of the guidance suggested that this narrowing of scope is intended to be permanent, and in fact, Part 11 no longer applies to all electronic manufacturing data. It's now interpreted to apply only to those records and signatures needed to comply with FDA regulations. Additionally, the use of computer systems in the generation of paper records does not necessarily trigger Part 11.

The final guidance states that Part 11 only applies to four categories of electronic data; FDA required records that the manufacturer opts to maintain in electronic format in place of paper format; FDA required records that are maintained in both electronic and paper formats, where the electronic records are relied on to perform regulated activities; Any records submitted to the FDA in electronic format; and any electric signature intended to be the equivalent of a handwritten signature required by the FDA.

The key to identifying Part 11 records is in identifying actual business practices related to the use of electronic data. Automation systems, project planning, or systems validation projects, clearly identify the intended use of any electronic data, and identify it as subject to Part 11 or not subject to Part 11. One of the things that we see as a repeating theme out there is what the FDA wants is to know that you thought about things.

So you need to either say that we have thought about it and we're including it in our Part 11 compliance plan, or we have thought about it and we are not including it in our Part 11 compliance plan and for the following reasons. They're looking for logic. The intention should be formalized in SOPs that describe quality control practices related to automated systems.

So what didn't change? Well, there were no changes to electronic signatures. No changes to the electronic record clauses related to the system access controls or enforcing sequence steps. No changes to open systems, and no changes to signature and open systems. So one of the things that did happen recently was that in 2007, this guidance for industry, "Computerized Systems Used in Clinical Investigations" was released in May 2007, and this actually has some language in it that is also related to Part 11. And that's kind of our latest guidance on this.

So 21 CFR Part 11, as a brief overview, effective organizations include viral pharmaceuticals, human and veterinary personal care products, medical devices, and food and beverage industries. Part 11 applies all over the place, as you can see, through GLP, GCP, and GMP and affects a very, very wide variety of different types of systems.

One of the things that is notable is that there are Part 11 training requirements that are now ubiquitous in life sciences companies. Please note that SyberWorks is a provider of 21 CFR Part 11 training material and, so, if you're interested in finding a way to do a cost effective software-as-a-service e-learning system for Part 11 that would certainly be someplace to look in to.

Going back in the background a little bit again, CFR obviously stands for the Code of Federal Regulations. Basically, ever since the information revolution of the mid-1980s, every aspect of regulated business, be it food, pharmaceuticals, laboratory, biotech or medical device, is touched in one form or another by computerization. Trust is placed in these machines that aid the process that create, store, and retrieve information. Information has always been of vital importance in its physical form, and it also is important in its electronic form. And it's a huge asset to any organization.

So one of the questions that comes up a lot is, "What's the difference between Part 11 and GAMP?" Just to touch on that briefly, GAMP is a guideline; in Europe the International Standards Organization has a number of guidelines for regulated and non-regulated industries, which are considered helpful suggestions in order to achieve a mark of approval, such as the CE mark, that represents the standard of excellence in their production and their processes.

Businesses, wholesalers, and the public avoid commodities without that mark, yet within the United States, 21 CFR Part 11 is law and it's enforced by the federal government. The FDA is concerned with record falsification. Life science organizations that move from paper to electronic records while complying with Part 11 can significantly increase the efficiency and speed of the drug development, approval, and production life cycle.

Also there's a relationship between Part 11 requirements and security best practices with benefits including faster and more efficient FDA reviews and approvals of FDA regulated products; improved ability to analyze trends and problems, which can enhance internal evaluations and control; reduce costs of storage and control of record; and improve data integrity and accountability controls, which can lead to better protection of intellectual property.

Part 11 can be broken down into a number of different elements for both electronic records and signatures. The electronic records can be divided into two sections; technical, which should be considered application-specific, and procedural, which generally means that there is more of a general problem.

The guidance states that the agency intends to exercise enforcement digression regarding specific Part 11 requirements for validation of computerized systems. Although people must still comply with all applicable predicate rule requirements for validation, this guidance shouldn't be read to impose any additional requirements for validation. Validation and the extent of validation of computerized systems should consider impact the systems have on your ability to meet predicate rule requirements.

Your approach to validation should be on a justified and documented risk assessment and a determination of the potential of the system to affect product quality and safety, and record integrity. And this movement toward the whole risk-based approach is, I should hope, no news to anybody out there. What the FDA expects is a justification on whether or not to validate a system and that should be based on a documented risk assessment for all computer systems that are not validated or not fully tested. With that in mind, it's important to define risk categories for computer systems.

As an example, the standard approach is high, medium, and low. And for each validation phase define the extent of validation for each risk level. Assign each individual computer system used for GxP applications to a specific risk level and define validation steps for each individual system. We also recommend developing a procedure for consistent implementation.

The final guidance describes specific approaches to reducing the stringency of validation, audit trail, copies of records, and record retention requirements. Importantly, it's now the case that complying with Part 11 requirements can now, except in the case of copies of records, be justified through a documented risk assessment. Of course risk should be interpreted as risk to public health and safety and you need to be able to prove the quality of your product. That's really the goal. The public can not be at risk. So again, you have to be able to prove the quality of your product. That's the goal.

It's important to understand that the focus of risk-based compliance strategies is a comprehensive initiative for the FDA. It's also important to note that the new FDA commissioner has stated that the leniency of the past eight years will no longer be tolerated, and that enforcement is intended to be swift and visible. This was just out in August 8th. There was an announcement by the new FDA commissioner who outlined a six-point plan for the new approach to FDA enforcement.

And among those things the time from an observation to a response has been narrowed from, it used to be 30 days and now, it's 15 days. So, I think, what we're going to see is a lot of enforcement happening pretty quickly. I don't actually, personally, think it's a surprise that it was accidental that Pfizer's \$2.3 billion fine came just one month on the heels of the FDA commissioner being appointed.

Predicate rule requirements provide governance for most industry regulatory activities within life sciences organizations. Predicate rules are preexisting regulatory requirements that include GLP, GMP, and GCP guidelines. These requirements are essential to Part 11 in that they provide the ground rules for management of electronic records produced in accordance with Part 11 guidelines. It's important to understand the risk associated with documents required under current predicate rules and incorporate this risk assessment in the development of Part 11 compliance systems.

Inspectability ensures that systems will produce hard copy information that accurately reflects what information is held in the application. It's also intended to ensure that records throughout the record retention period are archived and can also be retrieved. The agency wants to be able to trace final results back to the raw data using the same tools as the user had when this data was generated. This is probably one of the most difficult requirements to implement because, in some ways, it does require a fair amount of interpretation knowing that in some instances, the records have to be kept for 10 or more years. In some cases, we've seen records that companies will keep for 30 years. As computer hardware and software have such a shorter lifetime, there's a variety of different problems that are associated with that. How are you going to store this data?

Also, an extremely important factor in maintaining data integrity and eliminating record falsification is security. How secure is the access to the data, both physically and logically? Data security and data integrity remain critical IT issues. After all, this Part 11 electronic records are replacing paper records, and electronic data can be pretty vulnerable. Putting controls and safeguards around the electronic data can be also fairly complicated. Limiting access can be ensured through - you guys, have all heard this - both physical and logical security mechanisms.

Many companies already have procedures in place. We recommend certainly putting them in place yourself, if you don't have them. For logical security, users typically log on to a system with the user ID and password. Physical security through locks or pass cards, in addition to logical security, is recommended for high-risk areas. For example, data centers with network service and backed data. This procedure should be very well documented and validated.

If records are changed, we need to know that they have been changed, when, and by whom. The objective here is to ensure and prove data integrity. If the data is changed, the computer should record what changed and who made the change. The audit trail functionality should be built in to the software, and, especially important for critical computer later processes, with manual operator interaction. Audit trails are requirement of some FDA predicate rules, including 21 CFR Part 58. If the audit trail isn't generated by the computer, it should be generated manually as a minimum. A record's integrity is a basic requirement of regulations, especially for critical records. It's difficult to demonstrate record integrity if there is no electronic audit trail, and it's critical where any change of data could have an impact on critical records.

Procedural elements are ones where many organizations fail, regrettably, and it's here that Part 11 encroaches onto Part 820. Qualification is the same for automated systems as well as manual systems. One of the basic questions is, have the users been trained? Typically, they have, but unless you show evidence to the fact, it means nothing during an audit. Here, again, I recommend looking at something like the SyberWorks Learning Management System where you can have a Part 11 compliant training management system that will support having a full audit trail of everyone that's been trained and keep the records permanently. Other situations concerning the hunting of these training records, and it takes time just like a control, and control is the main element in any FDA audit.

Accountability is, basically, writing down procedures showing who is responsible for what. How often does it occur where procedures are in place but not being followed? That's a really, really common thread of FDA 483s. Better not to have a procedure at all. If there's a weakness here, then the weakness shows like a fissure all the way up to the quality management system. This area is also potential for bringing weakness up within the document control system. If there's a weakness, then documentation could also be a problem. With documentation, here, we should be able to show control over any manuals, quick start guides, user help guides. If it's weak here, it could show up weakness in document control or a lack of adherence to procedure.

With respect to open and closed systems, more and more corporations are centralizing their systems, even on a global basis. This could constitute an open system if you've got, for instance, a data farm that serves your entire organization on a global basis. Example of an open system is one where, for example, the data is stored on a server and is under control of a third party. The other obvious example of an open system are websites where everybody has access. Contrast that with the closed system. One of the examples that I would like to use is like the Internet as opposed to the intranet. Often, companies will have an intranet with all the HR policies and a variety of other things on them, and that's a closed system because you can't Google it from the outside.

It's important to ensure the same compliance issues where the closed systems that we have just covered. It's also important to ensure that the system provider is held accountable for the protection of the data contractually. If you're outsourcing your data to be hosted somewhere else, you are responsible for ensuring the data is protected. Nearly all

systems in labs, for instance, are closed systems. Typically, without a security system in place, labs have full control on who will access their systems.

Electronic signatures are the electronic equivalent to handwritten signatures on paper. They can be based on biometric methods like fingerprint scanners or a facial and voice recognition or simply, on a combination of a user ID and password. Within a company, a user ID must be unique to a specific person, electronic signatures are sufficient for closed systems. Procedures have to be in place to maintain control of who has the authority to use electronic signatures, to show handwritten signatures against their username which also confirms an understanding by that signatory of the implications and ramifications of using their electronic signature.

Generally with electronic signatures, it's here where policies and procedures are very advisable, and people need to be extremely clear of what it is that they're expected to do. The most common form of electronic signatures is simply a combination of a user ID and password, those are your non-biometrics. And electronic signatures that are biometric, I already mentioned them earlier, retinal scans, fingerprints, facial and voice recognitions are the common ones these days.

With respect to identification codes and passwords, this can be utilized for either physical control of a piece of equipment or a process, and it's also the guideline for remote access to a system.

Linking electronic signatures to relevant electronic records and the signer of the records means that the signer should be recognized by the system through user ID and password, and procedures and technical control should ensure that the signer is uniquely identified. This definitely requires not only the development of procedures, but even more importantly, behavioral changes on using ID codes and passwords. It's something that you really need to teach your users and enforce it and make it habit-forming in the group.

Part of the reason for that is that, regrettably, it's a lot less challenging for someone to think about sharing their user ID and password on a computer than it is to say, hey, can you forge my signature. They just carry different levels of sort of a moray against doing that. However, the important thing is that under Part 11, forging a signature on a piece of paper or using someone's user ID and password, it's the same consequence. It's considered exactly the same thing.

There are a lot of interpretations of Part 11 compliance available with software vendors, consultants, IT managers, business managers, many of them all interpreting it differently. Also, the compliance requirements for one organization can be totally different from that of another organization. A classic example that we have is a client that was just acquired by a Fortune 100 firm, so we have a small company of 200 people that was just acquired by, you know, a global Fortune 100 firm, and while the requirements for Part 11 compliance were at one level for this startup of 200 people, as soon as they were acquired, now they were measured against the mature policies and procedures that this global company had. And so they had to do a complete remediation of all of their validations, including all of those related to 21 CFR Part 11.

It's highly recommended in these situations and as you're going about doing your Part 11 compliance projects to utilize experts with GxP experience to help bring consensus on how Part 11 should be interpreted for your particular compliance projects. We always recommend that folks do what's appropriate for the size of their organization. It's common to go overboard, and what you want to do is have your approach to validation be robust and defensible, but also at the same time minimalistic. You should be able to stand proudly in front of the FDA and defend what you have, but you don't want to spend money where you don't need to.

Write your interpretation down and communicate that throughout your organization to ensure a common understanding. So, one of the first things that typically happens is that you decide that you're going to do your Part 11

compliance project, and then you come up with an interpretation of Part 11 that's adequate to meet the needs of your environment. Compliance with 21 CFR Part 11 then means that policies and procedures exist that you'll have to create to help ensure the development, deployment, maintenance, and use of validated computerized systems, and the establishment and maintenance and accountability for activity regarding electronic records and signatures. There's a lot of different roads to compliance with Part 11. Again, I recommend leveraging experts to help support that.

Part of the typical process of going towards Part 11 compliance involves doing a whole systems inventory. You have to develop an inventory of your hardware and software and a network architecture document appropriate for your circumstances. This is the basis for your compliance. You need to know what you have and where it's located.

During the stage of doing a systems inventory, you'll be developing a master plan and SOP for risk assessment. You'll also determine the risk category for each system. If you don't have one, I'd recommend picking up a copy of GAMP 5, which offers a good risk-based approach to compliant GxP computerized systems, and it really addresses the types of software systems that are out there in common usage today.

As you move forward identifying the computerized systems in your inventory, you'll need to continue your process of becoming Part 11 compliant by defining a priority schedule to bring all computer systems into Part 11 compliance. There's often not just the potential risk to human health and well-being, but also there's business decisions that need to be made in this stage as well. And during this part, you develop a procedure on how to define Part 11 controls and also define Part 11 requirements for each system.

The gap analysis is essentially the gap between your existing environment and CFR Part 11 standards, and it results from your systems inventory. Once the gaps are identified, prioritize the applications and business processes which are to be made compliant based on their functionality and business predicality. The deliverables at this step should include a list of systems requiring compliance, prioritization of systems based on issues like data integrity and the extent of compliance, a detailed action plan for each of the identified systems, and resource and project plan for remediation. You have to remember that this is the stage where you are going to be leveraging your existing staff and potentially consulting staff. You have to do your resource loading requirements, determine what bandwidth your existing staff has to participate in a remediation effort.

The deliverables of the gap assessment will include: the list of systems requiring compliance; the prioritization of the systems based on issues like data integrity; the extent of compliance required, etc., a detailed action plan for each of the identified systems; resource and project plan for remediation.

Doing the gap analysis to determine a missing functionality in procedures for systems and developing an implementation plan to bring systems into Part 11 compliance.

You need to estimate the costs for the systems and for the project as a whole. You also need to develop procedures for limited system access to authorized individuals, which of course should include your password policy.

You then come to the point of doing remediation, which is what happens after you've gotten your whole gap assessment report completed and you've created your validation plan. Based on the gap assessment requirements for code changes and testing are identified and detailed implementations of remediation efforts begins to be carried out. The remediation planning needs to consider the speed at which your company can remediate the systems, the time available to remediate all of the affected systems, the availability of the application and systems experts who helped design the systems to assist in the remediation process, change management issues, level of risk your organization is willing to assume and preparation of back-up and contingency measures, to ensure continued reliable service to customers, both during and after the Part 11 compliance process.

Eventually, the result of going through a whole Part 11 compliance initiative takes you to the part where you are then maintaining compliance. Maintaining compliance is essentially the point where procedures and controls that are designed to ensure the authenticity, integrity and, when appropriate, the confidentiality of electronic records and to ensure that signers cannot readily repudiate signed records as non-genuine. That's where you get when you are at the point of being essentially done with your Part 11 compliance project.

And it's at this point that we're ready to take some questions.

Mary Kay: Park, there seems to be quite a lot of questions there, so.

Park: OK. So, I just need to be able to get to them.

Mary Kay: Go to the questions area.

Park: Yeah, sorry, guys. I'm not an expert at this thing.

Mary Kay: Alright. That's fine. I'll read you one. How about that?

Park: Alright.

Mary Kay: OK. Here's one from Larry. It's, "Are open source code systems, by their very nature, not compatible with 21 CFR Part 11? I've heard conflicting statements from learning vendors that offer modal."

Park: Open source code systems can be made Part 11 compliant. The trick is that you have to cease the code once you've done your validation. So, there's a difference between an open system and open source code. Open source code means that the code that a system is written in is something that it goes to revisions by different people who are, you know, different coders who are out there. Once you've brought a system that is an open code system into an environment, if you go through the process of validating it, you're basically going to be storing the source code into a secure source code safe. Once it is stored in that location you cannot make any revisions to it. You cannot have anybody get into that code, or you will be invalidating the validation that you've done on that system.

So you can use it, but again, just like any other system, once its gone through the process of going through the validation plan and all the various testing phases, IQs, OQs, PQs, etc., and doing the traceability report, at that point you have to lock the code down and put it in source safe and not touch it. That's really what the definition of doing validation is. And this is why, for example, when you're doing any system... Let's say that you're using an Excel or let's say that you're using TrackWise, a common system. TrackWise, you bring it into your environment, and you lock it down when you do the validation. Once you're finished with the validation, it stays in that locked state and it stays in a compliant state. But as soon as TrackWise releases the next stage of their software, or the next iteration of their software, well, now you're bringing in new code so you have to revalidate.

Mary Kay: Well, yes, there's also other business issues associated with open source, too. Alright. Here's another one, Park. "Are logins with password control adequate to meet Part 11 requirements for traceability?"

Park: So long as there's a full and complete audit trail, yes.

Mary Kay: OK. Alright. Let's see.

[pause]

Park: I see one thing here that I'll just go ahead and state. Yes, the slides will be made available. I'll be PDFing these and shooting them out shortly after the presentation today. You'll have them before the end of the day.

Mary Kay: OK. Go ahead. Here's another one, Park. It says, "For hybrid systems and systems where the computer prints out a hard copy record and the hard copy is considered the document of record, how does one decide whether the system must be validated or not?"

Park: That's a good question. I don't actually know the answer to that off the top of my head. There's so much to know about Part 11 that it's difficult to know all the answers to all the questions. I've gotten volumes of literature on this and I know that I have the answer to that but, to be honest with you, I was up late last night and I just don't remember the answer to this question right off the top of my head. I'm sorry.

Mary Kay: No problem. So, I think we will just wrap up from here.

Park: Yeah.

Mary Kay: Don't worry, I'm sure Park will be getting the answer to that question and all of these questions. We'll be sending out the answers on a questions and answer document, so you'll get that information. Again, this is Mary Kay Lofurno from SyberWorks and I just wanted to mention at the close that one thing Park mentioned is that SyberWorks does provide a GxP compliant 21 CFR-supported learning management system that can be purchased as software-as-a-service, and license. So, it certainly works in a closed system. There was one of those questions that came up about that as well. So we'll be sending out a survey after the conference so we can understand what was helpful and so we can learn more about it and get some information on future topics.

Join us again on December eight at the same time of day for our next webinar on quality systems and CFR 820. Look for the upcoming announcements covering the details and registration. We hope this webinar was informative and you enjoyed the presentation. Have a great day.