

IncidentMonitor and Title 21 Code of Federal Regulations (CFR) Part 11 for Electronic Records and Electronic Signatures (ERES)

Prepared by
Monitor 24-7 Inc.

February 5, 2015



Background

Title 21 CFR Part 11 is the part of Title 21 of the Code of Federal Regulations that establishes the United States Food and Drug Administration (FDA) regulations on electronic records and electronic signatures (ERES). Part 11, as it is commonly called, defines the criteria under which electronic records and electronic signatures are considered to be trustworthy, reliable and equivalent to paper records (Title 21 CFR Part 11 Section 11.1 (a)).

21 CFR Part 11 sets out the procedural and system requirements for controlling and auditing electronic records and signatures. These controls include User Authentication, System Access Controls, Security, Audit Trails, Records Retention, End User Training, and Systems Validation.

More information regarding this can be found on the FDA web site looking for Part 11, Electronic Records; Electronic Signatures — Scope and Application.
(<http://www.fda.gov/RegulatoryInformation/Guidances/ucm125067.htm>)

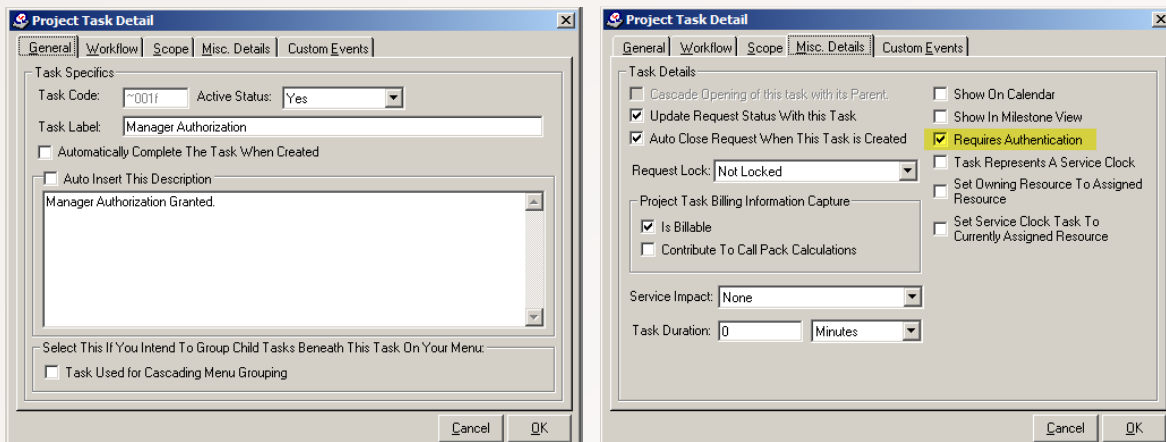
Overview

This whitepaper will go over some of the features within IncidentMonitor™ that will help your organization achieve compliance with regulators.

User Authentication

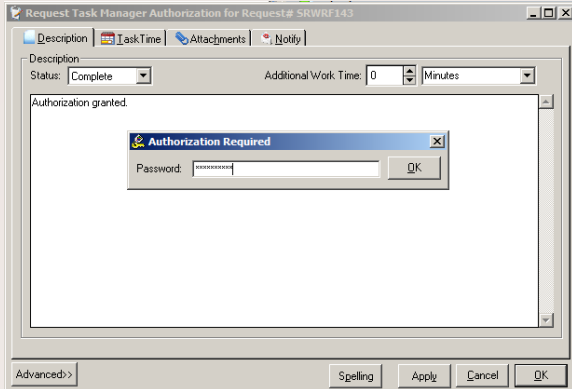
IncidentMonitor™ uses just about any secure directory service to authenticate users. In addition, IncidentMonitor™ has its own directory service that can be used if you don't want to integrate it with your directory service.

User authentication is used for the both validating whether or not a user has access to the system in addition to certifying any authorization granted by a user was actually performed by them. Any step within a process can have the Authorization Required property enabled which causes IncidentMonitor™ to challenge the user for their credentials in order to validate that it is actually them performing the action, prior to saving the information. If the authorization fails the system never saves the information. The definition of the task would be as follows:



The image displays two screenshots of the 'Project Task Detail' dialog box. The left screenshot shows the 'Task Specifics' tab with the following fields: Task Code (~0011), Active Status (Yes), Task Label (Manager Authorization), and a description box containing 'Manager Authorization Granted'. The right screenshot shows the 'Misc. Details' tab with various checkboxes and dropdowns. The 'Requires Authentication' checkbox is highlighted in yellow. Other visible options include 'Update Request Status With this Task', 'Auto Close Request When This Task is Created', 'Request Lock' (Not Locked), 'Is Billable', 'Contribute To Call Pack Calculations', 'Service Impact' (None), and 'Task Duration' (0 Minutes).





Now whenever a user tries to perform the Manager Authorization step on a request they will be prompted for their password. The system will take their already provided user ID along with the password entered and then verify it against their associated name space. If everything is correct then the step will be performed. If the information is not validated the step is not created.

Even if a user left their workstation unlocked and in the application, it would be next to impossible for them create the Manager Authorization

unless they know the user's password.

System Access Controls

All access to the system is audited so you always know who accessed the system, from where, using what software and how long their session was active. The system also interrogates any request it received to ensure it doesn't contain any hacks that are typically used (e.g. cross site scripting, SQL Injection etc). If any request looks suspicious the action will be logged and the packets will be dropped.

All data and audit-trails are stored in a secure SQL Server database requiring administrative access rights to see the data. The database is accessed via the SQL Server Native Client driver and Open Database Connectivity (ODBC) industry standards.

IncidentMonitor™ also implements another layer of access control using a feature called data access validation checking. For example, let's say you have two projects on your system (clinical trials and building maintenance). Users need access to their projects however you only want them to be able to access their own projects. IncidentMonitor™ does this project access control no problem by default. However, you want to make sure that even if a user in the other area can't use their session credentials to take a web page request and change the information such that it targets the other project. IncidentMonitor™ would receive their attempted request for the other project and once it performs the data access validation testing it would determine that they are trying to access data that isn't theirs. This attempt would be denied.

Security

You must first be able to pass through all of the network security before you can even communicate with the IncidentMonitor™ system. If you pass through that layer then there is a complete role based security system implemented within IncidentMonitor™. This allows you to control all aspects of access to data and actions on the system. IncidentMonitor™ can leverage your existing directory service for authenticating users or even leverage its own directory service.

It doesn't matter how you connect to the IncidentMonitor™ system (web services call, XML, COM+ interface, browser, wireless, Windows client software etc) you always have to generate a session with the system (login to the system). The session token generated can only be used by you from the device you generated the session from. Meaning someone couldn't put a network sniffer on your physical network or wireless network and then try to use the session from another device.



Records Retention

All critical data is fully audited so you can see the previous values and the new values. Even if data is deleted it is only logically deleted. Meaning, the data is still on the system in the audit trails such that you could recreate the entire request from the audit trails.

IncidentMonitor™ was designed and optimized to store large amounts of historical data such that it doesn't really impact the accessing of current data. This allows you to meet any kind of retention compliance requirements but still have an optimally performing system.

End User Training

IncidentMonitor™ provides online training videos and an online user guide for reference on how to use the software. Due to the fact that the system has a full electronic forms designer and workflow designer, users can design just about any kind of process or service catalog. In cases such as this the user would create their own training content.

Systems Validation

We follow a standard system methodology for documenting system requirements, system design, test plans (unit testing, functional testing, integration testing, performance testing) and coding standards. A large amount of our software code is generated using modeling tools that leverage our 30+ years in perfecting our code generation templates.

A complete change control system is used to track all changes and associated documentation. Our facility that houses all of our data adheres to physical access control procedures as well as network access control procedures.

Conclusion

We have gone over a few of the areas regarding features of IncidentMonitor™ that will help your organization achieve compliance with the regulation bodies in your industry.

A Final Word About IncidentMonitor™



IncidentMonitor enables you to easily adapt to the needs of your organization. With its configuration capabilities and unique project concept you are able to start with a

simplistic linear request management system and grow this over time. We see many implementations start with a simplistic Incident Management approach which simply aggregates all of the out-of-band (i.e. e-mail, chat, web requests, etc.) and in-band data (service requests, incidents, change requests etc.) into a single system for reporting and statistics. Then as the organization matures (by organization we mean your service organization and your end user community) other aspects are turned on (or enabled).



About Monitor 24-7 Inc.

Monitor 24-7 redefines service management by helping organizations improve their customer-facing functions. Monitor 24-7 provides simple solutions that tackle complex help desk processes -- right out of the box. Our goal is to help customers reduce running costs, manage change, implement a fully functional advanced software solution and lower the cost of ownership.

Monitor 24-7 is a software development organization focused on service management. Years of experience and many different customers have brought us where we are today. We believe we have proven ourselves and we are very proud of our flagship IncidentMonitor -- an enterprise service management solution which is being used in many different environments.

- 100% dedication to Service Management since 1999
- Over 250 customers, more than 10,000 licenses sold
- Active in 10 countries

Monitor 24-7 Inc Head Quarters

335 Renfrew Drive Suite # 301
Markham ON
Canada
L3R 9S9
Phone +1 416 410.2716 / +1 866
364.2757

sales@monitor24-7.com
www.monitor24-7.com

Monitor 24-7 Inc Europe

Zijlweg 142-L
2015 BH Haarlem
The Netherlands

+31 88 008 4601

eusales@monitor24-7.com
www.monitor24-7.com

