WHITEPAPER

Choosing

Commercial off the Shelf

(COTS) Software Licensing for Medical Devices and Applications

Introduction

As technology continues to evolve, and the environment of the medical industry is more connected through IoMT (Internet of Medical Things), the chances your medical device has a software component is extremely high. Even medical devices whose intended use does not directly require software, will necessitate a software component to be a part of a connected ecosystem. Many medical device and medical applications manufacturers are considering Commercial off the Shelf (COTS) software that is available rather than using internal resources to develop software from scratch. In this paper, we focus upon software that is Commercial off the Shelf (COTS), which means that it is software that can be purchased, leased or licensed from a third-party vendor. A software being Commercial off the Shelf (COTS) does not refer to how the software can be licensed. COTS software can be licensed however the software developer chooses, which includes offering the software under an Open Source license, a Commercial license, or both. The business decision as to what software will be developed internally and which will be acquired off the shelf is not trivial and made very strategically.

Once the decision is made as to which software will be used commercially off the shelf, the focus then turns to what software licensing best fits the medical device manufacturers' business model.

Open Source licenses
Depending on licensing type: parts or all code are to be shared forward
Some of the requirements for using Open Source code will pose direct or indirect costs or other obligations
End user is allowed to use one or more copies of the software

Commercial software
Source code is "locked-down"
No requirement to share code
End user is allowed to use one or more copies of the software
License requirements are set by the company developing the software

Many companies, when selecting COTS software, will focus on the fact that Open Source software typically comes free of charge. With the constant pressure of keeping costs to a minimum, this becomes very enticing; however, all Open Source licenses have requirements for the users, and those requirements might pose either direct or indirect costs or introduce other obligations.

For a number of medical device developers, choosing to enter into a Commercial software license over an Open Source license might be a better choice despite the fact it costs money. The financial burden of purchasing this type of license may outweigh the risk or requirements associated with Open Source licenses.

Open Source Licenses Overview

As mentioned in the previous section, different types of Open Source licenses carry with them different requirements to share the software code, and any modifications to it, forward. Many companies focus on the "free" aspect of the license and fail to understand the differences between the Open Source software license types. These differences can greatly impact one's business and a common mistake of generalizing all Open Source license types should be avoided so that the best decisions for one's business can be made.

There are several different types of Open Source licenses as defined by the Free Software Foundation (FSF). A list of the licenses with links to the latest version of the license are as follows[1]:

- **GNU General Public License (GPL)**
  - GPLv3, GPLv2, GPLv1
- **GNU Lesser General Public License (LGPL)**
  - LGPLv3, LGPLv2.1
- **GNU Affero General Public License (AGPL)**
  - GNU AGPLv3
  - The Affero General Public License version 1 is not a GNU license, but it was designed to serve a purpose much like the GNU AGPL's.
- **GNU Free Documentation License (FDL)**
  - FDLv1.3, FDLv1.2, FDLv1.1

For the purposes of this discussion we will focus upon the popular GPL and LGPL versions of the Open Source licenses.

1 https://www.gnu.org/licenses/licenses.html
GNU Operating System, Sponsored by the Free Software Foundation

Designing Medical Devices with Open Source vs. Commercial licensed Software

A common misconception is that because outside interests can contribute to the development of Open Source licensed software, there is a lack of control in the development process itself. This is not necessarily the case. While software firms manage their own software QA processes, and can manage them differently, Open Source licensed software should be validated and tested the same as Commercial licensed software. For example The Qt Company has a multi-licensing model and offers both Open Source licensed software versions and Commercial licensed software versions. In both the Open Source and Commercial versions, contributors from inside and outside The Qt Company participate in the development of future generations of the software. Every contribution is not necessarily accepted and is subject to formal review with mechanisms in place for tracking and governance of what goes into subsequent versions of the Qt software. Prior to each release, both the Open Source version of Qt and the Commercial version of Qt are fully tested and validated against the specification, maintaining its history of being robust, reliable, safe, and secure.

One area where medical device manufacturers need to be concerned is what could happen once the medical device is delivered to their end user. One of the differences between Open Source licensed software and Commercial licensed software is what is required after the medical device is sold. As part of the LGPL Version 3 Open Source license, there is a clause in the licensing agreement that you, as the medical device manufacturer, must allow whomever you are selling or distributing the device to modify the software. This clause, dubbed the anti-tivoization clause, is the central focus of the LGPLV3 open source license. Version 3 of the LGPL Open Source license was written and released in response to a situation brought on by TiVo, the popular manufacturer of Digital Video Recorders (DVRs). TiVo used hardware with restrictions that blocked their end users from running modified software on a TiVo DVR box. Although this did not go against the LGPL Version 2 license which their software was under, this did go against the objectives of the FSF Open Source community.

Should you choose to use COTS software under a LGPL V3 Open Source license you are potentially putting the functionality, safety, and security of your device at risk. For example, the Qt Software Framework Version 5.9 is available under an Open Source LGPL Version 3 license and a Commercial license. There are features and functionalities that are available in the Commercial licensed Qt Software that are not available in the Open Source licensed software. Features and functionality aside, by allowing end users to modify the Qt Software running on your medical device under the LGPL Version 3 license, they are directly changing the behavior of the apps, device, and security built on the Qt framework. Changing this behavior puts your device's safety, security, and intended use at risk. In contrast, working with Qt under a Commercial license you are under no obligation to allow your end user to modify anything in the software. Your software can be locked down so that zero modifications can be made, thus mitigating the potential risks brought on by working under the LGPL Version 3 license.

Patent enforcement

A second area of concern for medical device manufacturers is how patent claims can be enforced. Both the Open Source GPL Version 3 license and LGPL Version 3 license contain explicit clauses to prevent people from attempting to enforce patent claims against other licensees of Open Source code. If a patent claim is made, commonly referred to as patent retaliation, a second clause explains how the person or entity making the claim would lose their Open Source license and any patent licenses that accompany it. In this situation, a medical device manufacturer forfeits their rights to patented software if it is bundled in a device or application with COTS Open Sourced GPL Version 3 or LGPL Version 3 licensed software. These patent clauses are complex so it is always recommended to go through them carefully with legal counsel to make sure this would not be an issue if deciding to use GPL Version 3 or LGPL Version 3 software. In most cases your software patents are safe and patent claims can be made if they are infringed upon when your software is bundled with COTS software under a Commercial license. The Commercial license requirements are made by the software developer; however, often with these types of licenses your software IP and patents are secure. Again, it is always recommended that Commercial software licenses are reviewed carefully with legal counsel to make sure whatever requirements the COTS software developer has are acceptable to you and your business.

When the final decision is made, depending upon what role the software plays in the design and functionality of your medical device, what software patents you hold, and what Open Source and Commercial licensing is made available to you, the choice to work under a Commercial license might be the better choice.

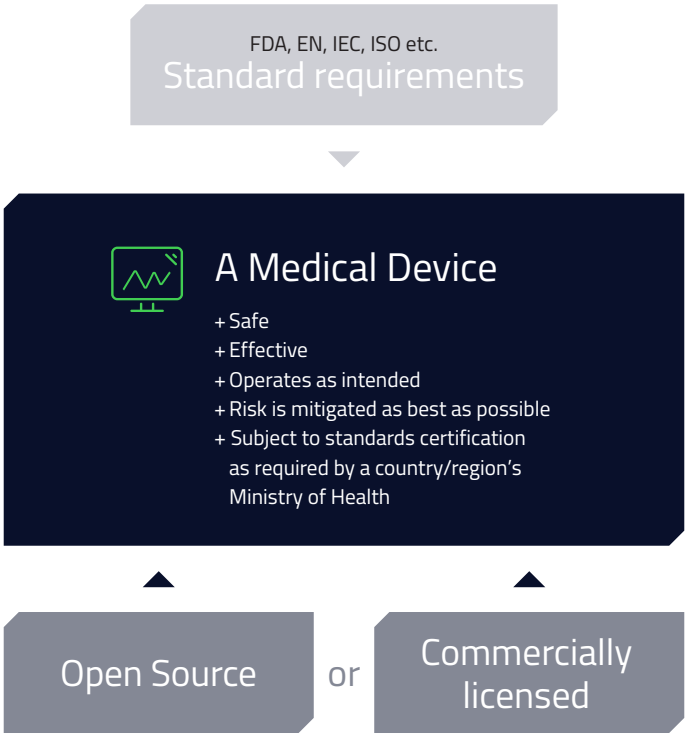
Medical Device Software IP management

When deciding upon the best COTS software licensing for your medical device, how your software IP is affected must be considered. Depending upon how your software code interoperates with the COTS software, there are certain requirements from an Open Source licensing standpoint that do no not apply in a Commercial licensing situation. If the software code you develop needs to integrate, make calls to, or somehow interoperate with COTS software code, it is typically accomplished through either dynamic or static linking. There is an ongoing debate regarding which type of linking is optimal as there are pros and cons for each as it applies to speed, performance, ease of updates, total resource consumption, etc. These are decisions that are made based upon functionality requirements and needs.

The other area to consider when choosing how you will link software is your responsibility to share and make code public when working with Open Source licensed software that is COTS. If you choose Commercial licensed software that is COTS, it doesn't matter how you choose to link it to your software. Regardless of dynamic or statically linking your software code to the COTS software, you are under no obligation to share either the COTS software code or your software code. Your IP is 100% safe and secure.

If you choose to work with Open Source licensed COTS software then you are required to share the COTS code and any modifications to it. How you choose to link your code to the COTS software might carry a requirement for you to share your software code along with the COTS code:

- If the COTS code is under a GPL license, you must share your software code and the COTS code regardless if you dynamically or statically link the two. Your software IP is at risk.
- If the COTS code is under an LGPL license and you dynamically link you code to the COTS code, then you do not have to share your software code but you still must share the COTS software code. Your software IP is safe. Functionality and security considerations still need to be weighed and decided upon.
- If the COTS code is under an LGPL license and you statically link you code to the COTS code, then you must share your software code and the COTS software code. Your software IP is at risk.



Software Licensing in the Medical Industry

The two areas of particular concern when considering the use of Open Source software in medical devices are information privacy (HIPAA compliance and HITECH compliance) and cybersecurity. Managing cybersecurity and the security of data has to do, in large part, with managing risk. In October of 2014, the FDA issued a guidance document "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices". Prior to a medical device achieving market clearance by the FDA or other global government agency, steps to mitigate cybersecurity and privacy of in formation risks should be considered during the product design and development stages. However, in 2016, the FDA acknowledged that risk mitigation in these areas needs to also be done after the medical device has been released for sale into the market. The FDA guidance document "Postmarket Management of Cybersecurity in Medical Devices" was issued on December 28, 2016. The FDA, as well as other similar healthcare government agencies, acknowledge that no situation is void of risk nor is the expectation that a manufacture 100% eliminates risk. There will always be risk of a software security breach. What is expected of the medical device manufacturer and other contributing parties is that risks be identified, assessed, classified and steps be taken to mitigate said risk. The FDA has identified that risk management needs to be done both premarket (before the medical device is approved for sale within the market) and post market (after the device is sold and distributed in the market).

Steps to avoid risk post market can be focused, in large part, to the decision of which COTS software licenses are chosen. As previously mentioned, when under an Open Source license, the responsibility for the manufacturer is to allow access to the code so that changes and modifications can be made. When software is Open Source and end users are allowed to change the framework on which they are developing, it becomes increasingly more difficult for the medical device manufacturer to predict, classify, manage, or mitigate risk. Every time an end user changes the software framework, they are essentially creating their own version of the software. Because of this, the potential the cybersecurity and information privacy risk is more uncontrolled and becomes higher. Increased cybersecurity risk potentially means increased patient and user safety risk. Increased information security risk means an increased risk to being out of compliance with both HIPAA and HITECH standards.

Conclusion

Choosing which type of software licensing for 3rd-party, Commercial off the Shelf (COTS) software used in the development of your medical device is an important one. There are pros and cons for choosing either Open Source licensed software or Commercial licensed software. Although Open Source licensed software is held to the requirements and responsibilities explained previously in this paper, how that software is managed and controlled is in the hands of the software developer. You as a medical device manufacturer must choose the software vendor, and the licenses (Open Source or Commercial) under which that software is governed, very wisely. It can be difficult getting past the "free" aspect of Open Source software, but as stated in this paper there are other responsibilities and non-financial costs associated with it.

At the end of the day, you must choose which software licensing is best for your business, for the standards to which you must comply and certify, and for the safety of patients, doctors, nurses, technicians and other end users of your medical device.

Open Source - Qt

- Free of charge – but rarely a $0 Cost of Ownership
- Community support
- Possibility to keep application private with dynamic linking
- Enable customers to relink the Qt libraries (also with static linking) (mandated)
- Provide copy of the license and explicitly acknowledge the use of Qt (mandated)
- Make a copy of the Qt source code available for your customers (on request)
- Usage of DRM according to LGPLv3 limitations
- Strong limitation on patents

Commercially licensed - Qt

- Company contract
- Community support
- Qt support helpdesk
- Access to commercial only features, benefits, previews etc.
- Possibility to keep application private
- Possibility to keep application private with dynamic linking
- Optional relinking to the Qt libraries (also with static linking)
- Optional copying of the license and explicitly acknowledge the use of Qt
- Optional copying of the Qt source code available for your customers
- All rights to make and keep Qt source code modifications proprietary
- No limitations of usage of DRM
- Possibility to create or include patented software

References

1. "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, Guidance for Industry and Food and Drug Administration Staff", U.S. Department of Health and Human Services Food and Drug Administration Center for Devices and Radiological Health Office of the Center Director Center for Biologics Evaluation and Research, October 2, 2014
2. "Postmarket Management of Cybersecurity in Medical Devices, Guidance for Industry and Food and Drug Administration Staff", U.S. Department of Health and Human Services Food and Drug Adminis tration Center for Devices and Radiological Health Office of the Center Director Center for Biologics Evaluation and Research, January 22, 2016
3. "Medical Device Manufacturers & Open Source Security Vulnerabilities", Chester Liu, Blackduck.com, Feb 13, 2017

The Qt Company develops and delivers the Qt development framework under commercial and open source licenses. We enable the reuse of software code across all operating systems, platforms and screen types, from desktops and embedded systems to wearables and mobile devices. Qt is used by approximately one million developers worldwide and is the platform of choice for in-vehicle digital cockpits, automation systems, medical devices, Digital TV/STB and other business critical applications in 70+ industries. With more than 250 employees worldwide, the company is headquartered in Espoo, Finland and is listed on Nasdaq Helsinki Stock Exchange. To learn more visit **http://qt.io**