

**LOGICPlus™ White Paper Series**  
**Produced By LOGICPlus™ Marketing**  
**Series II: System Security and HIPAA Requirements**



## **ADVANCED TRANSPONDER SECURITY FOR MOBILE STORAGE SYSTEMS**

## **LOGICPlus™ and the New HIPAA Requirements**

**Much has been written in the past few months about the Health Insurance Portability and Accountability Act (HIPAA) and its impact on the security of medical records. A section of the legislation addresses the privacy of medical records and this has caused great concern to many health care providers and other effected organizations. As with many far-reaching legislative bills, the concerns arise not from the specifics of the legislation but from the gray areas left unclear by the legislation.**

**One significant area of the legislation speaks to the need for security of Protected Health Information (PHI), but does not provide clear guidelines for the handling this information. As a result most health care providers and others effected such as insurance companies and claims processing companies are left to make many of their own decisions about what level of information security is appropriate.**

**While security for information handled and stored electronically can be a costly and complicated program requiring technical expertise and direction, security for paper based records is much more straightforward. Security for paper records or x-rays can be achieved by limiting access to the cabinets or mobile storage systems that house the materials and/or records.**

**Limiting access seems a “simple” enough concept, but in the often hectic and highly time sensitive world of medical records an effective but workable plan for access limitation may be anything but simple. In the past, records stored in a high density mobile storage system could only be secured through the use of key locks installed on the carriages or floor mounted plungers with locks attached. As an alternative one manufacturer offered a numeric keypad requiring the input of a complicated code string to activate a secured aisle.**

**Any mechanical locking solution meant re-keying was required when staff turnover occurred or access permissions changed. This is a costly and time-consuming process and far too often was ignored meaning security had been at best diminished and at worst totally compromised. This solution also meant that the pattern of secured aisles within a system could not be changed without removing the locking mechanisms or adding additional locks. Again this is a costly and inconvenient process. The security functionality in every LOGICPlus™ controller makes these problems a thing of the past.**

**Now let's look at the security functionality of LOGICPlus™ in more detail.**

### **Electronic Transponders vs. Mechanical Keys**

**The transponder is an electronically coded device that sends a specific signal to the receiving logic system in the carriage touchpad. A secured aisle can only be accessed if a designated transponder is used to open that aisle. Unlike a normal key that can be copied by any locksmith, the transponder cannot be duplicated without access to the special equipment and source code utilized by the manufacturer. Anytime a normal key is outside the direct control of the system administrator the key is subject to duplication and the result is a potential breach in security. A system administrator knows how many authorized keys are in circulation but has no way of knowing if any duplicates have been created. The use of transponders resolves this issue for the system administrator.**

### Electronic Transponders vs. Numbered Code Pads

Some systems offer numbered keypads requiring the user to enter a numeric code to gain access to a given aisle. While the numbered keypad avoids the key duplication problem, it is actually more susceptible to unauthorized “access sharing” than mechanical keys. To create a duplicate key requires the step of having the key duplicated. Numbered keypads require only knowledge of the number code. If in the rush of normal activity an authorized user decides to give an unauthorized user the code for convenience in a specific situation that unauthorized user now has access to the secured aisle forever. While this type of sharing is ill advised and in all cases a break with operating policy, system users readily admit that it occurs far too often in normal day to day operations. Using the transponder cannot stop unauthorized sharing but when a transponder key is “loaned” to an unauthorized user and then returned the unauthorized user no longer has access to the secured aisle.

### Multiple Access to A Secured Aisle

LOGICPlus™ allows multiple accesses to a given secured aisle. The diagram in Example 1 demonstrates this capability. In the example multiple transponders have access to several of the aisles in the system. This shows that the system administrator can decide to grant access permissions by individual employee or by work groups. In the example the green transponder might be assigned to the radiology department with one or more green keys being provided to radiology. The red transponder might have been assigned to a given member of the staff. The yellow transponder might be assigned to surgical nursing and the black transponder to the system administrator.

### Access to Multiple Aisles

Again using Example 1 we see that the green, yellow and black transponders have been given access to multiple aisles within the system based on their needs to access the information contained in those specific aisles. The black transponder for the system administrator has access to all secured aisles and the red and blue transponders can only access the specific aisle designated.

### Mixing Secured Aisles With Unsecured Aisles

Unlike other security systems, LOGICPlus™ does not require that all aisles within the entire mobile system or just a bank of carriages within the system be secured. LOGICPlus™ allows users to secure certain aisles while leaving other aisles open to unrestricted access. In Example 1 aisle 3 has been left unsecured. This feature is of particular value in smaller systems or facilities where the mobile storage units house a variety of materials. Unrestricted items such as general supplies can be stored in the same group of carriages as restricted information or materials and the unrestricted items can be accessed conveniently without the inconvenience of unnecessary security steps.

### Changing Aisle Security Permission Patterns

Many things can necessitate a change in the security permission patterns. New departments of staff members may need access to secured aisle. New secured aisles may have to be

established on a permanent or temporary basis. The number of aisles required for items restricted to certain staff or departments may grow or shrink.

The ability to quickly and easily change the secured aisle permission patterns offered by LOGICPlus™ places it far beyond other security solutions. The system administrator simply clicks the desired change on the configuration setting screen and the new or revised permission pattern is established. No special equipment or training is required. With mechanical locking systems these changes would mean re-keying at the very least and in many instances would entail replacement of the whole locking mechanism. The process is costly, cumbersome and limits use of the storage systems while the changes are being made.

The simplicity of making these changes with LOGICPlus™ makes the mobile system a far more flexible tool and therefore a far more valuable tool for system owners.

### Using LOGICPlus™ With Other Access Control Systems

Many healthcare facilities already employ access control systems such as card readers for general access control throughout the facility. The LOGICPlus™ controllers have built in Application Program Interfaces (APIs). This means that the controllers can be programmed to interface with these outside access control systems. Should a system owner wish to utilize the same outside access control systems for their mobile storage system the card reader or other input device can be installed on the mobile carriages to work as part of the general access control system. In this case the transponder is replaced with the new input process but the security functions are the same.

### Remote Access Control For Ultimate Security

In cases where system owners require maximum security for health records, the mobile storage system with LOGICPlus™ offers remote access. This means that the carriages can only be moved by a remote command from a computer. Touchpads are not installed on the carriages so unauthorized access is virtually eliminated. This feature can be of benefit where highly sensitive records or controlled substances are stored. Carriage movement is initiated by using the simple windows based command screen on the system administrator's computer. While this level of security may be beyond the needs of most users, it is a capability found only in the LOGICPlus™ controller system.

### Access History Reporting

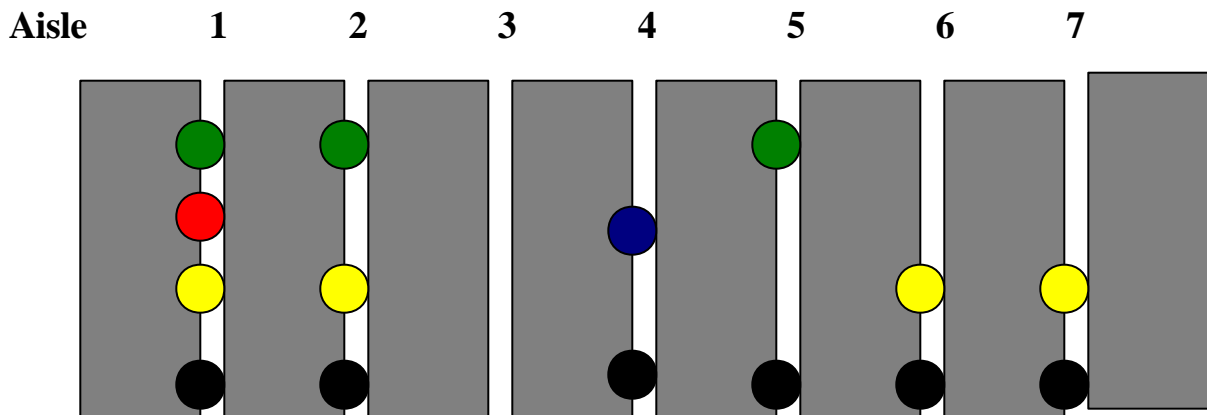
LOGICPlus™ engineers are currently developing a reporting package that will provide a detailed history report with user, date and time information. System owners will be able to add this capability on LOGICPlus™ controllers installed prior to the release of this advanced reporting capability.

### LOGICPlus™ In a Changing Environment

One thing is certain about HIPAA requirements. As time goes on the interpretations of the requirements, either set forth or implied by the legislation, will evolve and change. As a result, those making investments to comply with HIPAA requirements need to be assured that whenever possible they are buying flexible solutions that will continue to provide maximum benefit in this highly fluid environment. While currently recognized as state of the art, LOGICPlus™ is designed to evolve with additional functionality. This will allow

**LOGICPlus™ to meet emerging demands in the various marketplaces utilizing high-density mobile storage systems . High quality mobile storage systems offer years of performance. When those mobile storage systems include LOGICPlus™ controllers the storage systems become an asset that grows in value to it's owners and users as time goes on and increased functionality is added to the system**

## **Example 1**



### **Access Permission Pattern Example**

In the system security configuration shown above aisles 3 has no security limitation and would be available to any system user. Access to aisles 1,2,4,5,6 and 7 is limited to the designated transponders.

In the example the green ● transponder has access to aisles 1,2 and 6

In the example the black ● transponder has access to aisles 1,2,4,5,6 and 7

In the example the red ● transponder has access to aisle 1

In the example the yellow ● transponder has access to aisles 1,2,6 and 7

In the example the blue ● transponder has access to aisle 4