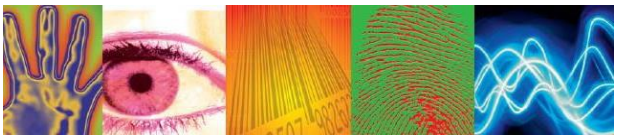


Biometrics and Hygiene Considerations

We have written this guiding document following concerns around biometrics and hygiene since the outbreak of COVID-19. It offers an overview of the issues around biometrics systems and hygiene, looks at the available research on the topic, and includes some questions and considerations that we hope will prove useful for your future decision-making.

What is hygiene?

When people are talking about hygiene, they typically understand it in terms of the proper washing and cleanliness of the hands, face and body.

What is poor versus good hygiene?

Poor hygiene practices can result in socially unpleasant outcomes like dishevelled hair and clothes, body odour, bad breath and greasy skin. They can also lead to more serious issues including the spread of germs, bacteria and viruses. In contrast, practicing good hygiene etiquette prevents the spread of unwanted disease and illness.

When and why do we need to practice good hygiene etiquette?

When people are sick and especially when they are coughing or sneezing, they need to take precautions [1]. These include avoiding close contact with others, covering mouths and noses with a cloth face mask when around others, catching coughs and sneezes in tissues and safely disposing of them, cleaning hands often and cleaning and disinfecting surfaces and equipment.

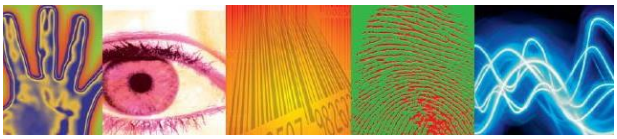
Good hygiene etiquette needs to be taken seriously in our everyday activities and business operations. This is especially important since many people are required to be in close contact with others and need to touch surfaces or operate medical or biometric systems that are regularly being touched by many people.

What are the general risks of using biometric systems?

As the use of biometrics in businesses and organisations becomes more prevalent, we also see the rise of concerns about potential risks, which may impact customers and employees. These risks include privacy, poor accuracy of systems, demographic differences in individual algorithms, ethical implications and human rights. Other risks include the resilience of biometric data processing systems – servers that process and store data – as well as workstations used to collect biometric data. These can be open to malware attacks, fraud attempts, data breaches and encryption. You can find links to our *Ethical Principles for Biometrics*, NIST reports on demographic differences and more further reading on these topics at the end of this document.

Are there hygiene-related risks when using biometric systems?

In light of the COVID-19 outbreak, we are reminded of the concerns around biometrics and hygiene. A good example is the use of touch-based fingerprint scanners. In these cases, people are asking,



"What is the risk of exposure from using modern biometric sensors?" and, "What is the relationship between the use of biometrics systems and hygiene?". For example, there are many travellers that have to go through security lines in airports [2]. These travellers can be asked to place one or more fingers or even their entire hand on a biometric scanner to quickly pass through immigration checkpoints. Unfortunately, shared contact with potentially contaminated surfaces can spread diseases to others. With touch-based biometric scanners, for example, finger, finger vein, palm vein and hand geometry, there can be a risk of transmitting pathogens – organisms that cause diseases – such as viruses, among regular users of the device.

While the risk can be reduced by adopting simple technical processes like using disinfectants, the follow up questions raised may be:

- How and how often are these systems being cleaned and de-contaminated?
- Are there any hygiene solutions available?
- Are they integrated already in existing systems?

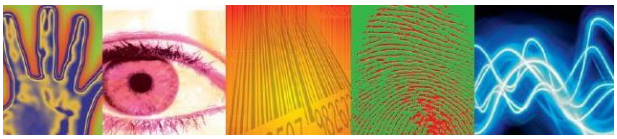
The problem is that certain pathogens, like COVID-19, can be transported only through droplets that are coughed or sneezed out directly from one human to another, or onto objects or surfaces. Also, preliminary evidence suggests that transmission can be airborne in certain circumstances. Therefore, we need to determine protocols and practices to reduce the risk of infection for all types of pathogens.

In the case of using biometric scanners and in particular touch-based scanners, can such pathogens be inactivated by heating the surface to a certain degree, or by applying UV light for a short period of time?

Future studies by experts will be able to better answer those questions that can help biometric practitioners develop the necessary hygiene-related operation procedures. In the meantime, another solution may be touchless fingerprint systems. Due to the scanning principle of such a system, the risk of exposure and disease transmission can be reduced. Finally, depending on the scenario and operational needs, considering other biometric modalities like face or iris may be preferable, since their sensors are not routinely touched by users and operators.

Contactless biometric scanners do mitigate the contact-based hygiene issues but present their own challenges. Facial recognition is becoming more common and, with people required to wear face masks to prevent the spread of airborne disease, we see potential impacts on accuracy. Facial recognition suppliers are retraining their algorithms and NIST has said it will perform an independent analysis to assess the extent of the impact as soon as possible. An impact is expected, given that a large portion of the face is unavailable to the technology when masks are properly worn.

Contactless fingerprint scanners are available. However, NIST's 2019 interoperability assessment, *Contactless-to-Contact Fingerprint Capture* [3] showed varying degrees of accuracy loss when comparing contactless probes against contact-captured galleries. The research found that devices requiring physical contact remain superior to contactless technology at matching scanned prints to images in a database. However, performance is improved when contactless devices scan multiple fingers on a hand. The accuracy impact is less on dedicated contactless scanners versus smart phone-based scanners but is still an issue. There are no FBI EBTS Appendix F [4] certified contactless



fingerprint scanners for forensic use, for example.

Whichever biometric solution you are using good hygiene practices may need to be considered.

Is the use of biometric scanners recommended when supported by hygiene practices – and how can the risk be reduced?

The hygiene level of biometric processing equipment can vary. This is due to possible pathogens that may be present from dirty or contaminated hands touching a four-finger flap scanner biometric device. Depending on the severity of the disease, this has the potential to be dangerous and lead to widespread infection.

Because some pathogens can survive better on some surfaces than others, their total elimination from biometric equipment and processes can be a challenge. So efficient control of disease at biometric processing units relies on good equipment hygiene, including good manufacturing and hygiene practices implemented by all biometric operators and users.

These hygiene-related practices and policies need to be effective, which means adopting:

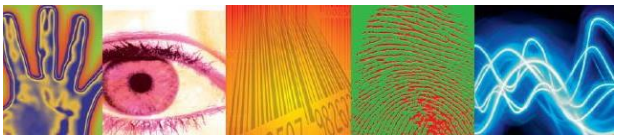
1. Procedures to decontaminate and rapidly detect contamination sources on biometric equipment, their housing enclosure or surrounding surfaces during operation.
2. Risk assessment procedures that support hazard analysis systems.

Therefore, questions to ask which may reduce the risk include:

- What are the recommended hygiene-related practices for operating biometric scanners? For example, do we need to implement disinfecting procedures, use heated surfaces, UV light or special anti-bacterial surfaces?
- Do we need to develop specific procedures for different types of biometric equipment? For example, how should our practices alter when using smart phones compared to biometrics kiosks?
- What processes – if any – do we need to consider around face and iris biometric sensors? The operational standoff distance can be high and also outdoors, including cameras placed in elevated positions that are not easily reached and touched by users and operators.
- What hand hygiene compliance procedures do we need to put in place? Studies on hand hygiene compliance of clinical staff has been identified as a major contributing factor to hospital-acquired infections [5]. Do the same risks apply when operating biometric sensors?
- Are policy changes required? While there are policies that address privacy or other risks, do these policies need to be re-structured or updated, considering the integration of hygiene-related procedures?

What is the latest research?

A search for “biometrics and hygiene” in Google Scholar brings back only a handful of articles. However, “equipment and hygiene” gives about 490 results as of April 2020. Outside an academic-focused search, there are many articles online that briefly mention the value of hygiene in biometrics [6, 7].



There are also some older academic studies which cover the subject of hygiene in biometrics. In 2007 Blomeke et al [8] discussed *Bacterial Survivability and Transferability on Biometric Devices*. The purpose of the study was to investigate bacterial (Staphylococcus aureus and Escherichia coli) recovery and transfer from three biometric sensors, namely a fingerprint, hand geometry and hand vein, and access the survivability of bacteria on these devices.

The study found that the bacteria could survive on an infrequently touched surface. However, a frequently touched contaminated surface was less contaminated within five to ten touches, as the bacteria was moved to the hand. The study also found that the amount of cells transferred with each successive touch rapidly decreased on the fingerprint sensor, while the hand geometry reader showed similar but less extreme results.

The authors state, "It is best for those touching common surfaces to wash their hands with soap and warm water on a regular basis" to remove the majority of bacteria from the surface of the hand.

In another hygiene-related academic study by Jacobs et al [9] in 2008, the authors concluded that touch-based fingerprinting procedures at that time are associated with a risk of infection transmission but if proper hygienic measures are followed the risk can be considerably reduced.

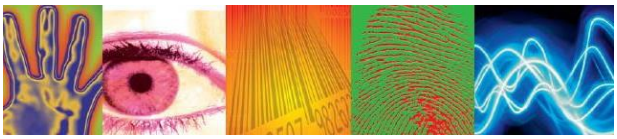
As discussed in *Hygiene not an issue for biometrics*, from 2007 [10] and *Biometric sensors no dirtier than doorknobs* in 2007 [11], biometric devices are usually repeatedly touched by many users and, "touching biometric sensors is no more harmful than handling a typical doorknob". Unfortunately, with the advent of COVID-19, this offers no reassurance as without good hygiene practices, the risks of infection and transmission are considerable irrespective of the surface.

Unfortunately, there aren't many papers on biometrics and hygiene and more research is needed. It will be beneficial to see studies on the risk of transmission of pathogens when using biometric devices under various conditions.

What questions should I ask about a biometric product that says it is hygiene oriented or hygiene proof?

The following questions are focused on contact-based devices that require the user to touch the biometric sensor like fingerprint, palm, signature and electrocardiogram (ECG). However, the questions can also be asked about contactless sensors, which can be accidentally touched during the process of enrolment or authentication [6].

As discussed above, shared contact with surfaces, contaminated with bacteria and viruses, are known to spread diseases to others. Having a contactless sensor does not mean that neither an operator nor a user can accidentally touch the surface of the sensor, its housing enclosure, or its surrounding surfaces during operation. As a result, it may be necessary to have hygiene-proof technologies and policies included in biometric sensor product operations, in scenarios where these sensors can be intentionally or unintentionally touched by a person.



Note: this does not apply to the use of biometrics sensors at a distance, like cameras used for face recognition, iris or gait. In these cases, equipment cleaning solutions are needed that guarantee optimal hygiene of the equipment.

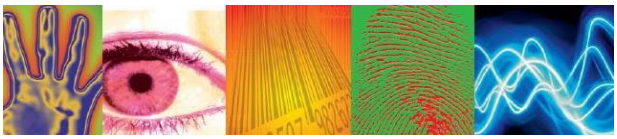
Questions

1. What hygiene-proof technologies does your product have?
2. Are there any hygiene policies included in your product operation?
3. Is there any hygiene-related training required for the personnel operating your product?
4. Does the biometric system use additional hygiene-focused hardware, software or material?
    - What controls are there to ensure there is no malicious code in the software either from the supplier or from any of the suppliers' subcontractors?
5. Have you conducted any hygiene-related analysis using your product?
    - Are there any white papers or additional information that can be shared around its use?
6. What hygiene-proof studies have you carried out? How did you evaluate the effectiveness of your system? What were the test criteria?
7. What is the complexity, cost and level of expertise required so that your product becomes hygiene proof?
8. If you have not already done so, can someone in your organisation or an independent contractor conduct a hygiene test on your biometric system?
9. What are the minimal hygiene requirements when operating your product?
10. Does your product follow any national or international hygiene standards or recommendations in terms of disinfection and cleaning, before and after each operation?

Adapting to a heightened hygiene-focused approach

Collaboration and ongoing discussions among biometrics users, engineers including sensor developers, and hygiene experts in academia, government and industry is critical following the disruption of COVID-19. In the meantime, good hygiene practices are essential for anyone using or operating biometric systems and could include:

- Applying simple hygiene practices in which biometric sensors, scanners and their housing enclosure can be cleaned with disinfectants.
- Considering providing and recommending the use of disinfectants to all biometric system users before and after each biometric capture.
- Considering the use of touchless or at-a-distance biometric systems, including touchless fingerprint scanners, or face, iris and other contactless biometrics.
- Recommending simple, hygiene-focused changes to social interaction among biometric system users and operators like replacing the standard handshake with the fist-bump in a biometric data collection and processing setting. This could help reduce transmission between operators and users by reducing contact time and total surface area exposed. A similar suggestion was made for healthcare settings [12].



Where can I turn for more information?

Biometrics Institute supplier directory

Search our supplier directory for a list of members experienced in biometrics systems in your field and contact them for independent risk analysis. Biometrics Institute members benefit from our request for information service which connects Biometrics Institute user members with experienced supplier members. Contact us if you have a specific request for information you would like us to send to our supplier members.

Biometrics Institute good practice material

The Biometrics Institute publishes good practice guiding documents which are available free to members. They include:

- Ethical Principles for Biometrics
- Biometrics Institute Privacy Guidelines
- Presentation attack detection and liveness
- Top 10 Vulnerability Questions
- Supplier members' response to COVID-19
- Contactless finger scanner solutions (living document)

References

[1] CDC on Coughing and Sneezing, July 26, 2016

[2] Enhancing Airport Security and Convenience from Curb to Gate, April 1, 2020.

[3] NIST's 2019 interoperability assessment, Contactless-to-Contact Fingerprint Capture

[4] FBI/CJIS biometric collection systems certified products list

[5] Teter J, Millin MG, Bissell R., "Hand hygiene in emergency medical services", Prehosp Emerg Care. 2015 Apr-Jun;19(2):313-9. doi: 10.3109/10903127.2014.967427. Epub 2014 Nov 21.

[6] Mohammed Murad, "Epidemics like coronavirus are putting a spotlight on contactless biometrics", Biometrics Update, Feb 19, 2020.

[7] Scanner cleaning , Integrated Biometrics

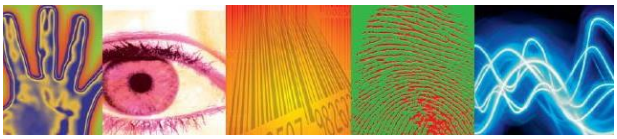
[8] C. R. Blomeke, S. J. Elliott and T. M. Walter, "Bacterial Survivability and Transferability on Biometric Devices," 2007 41st Annual IEEE International Carnahan Conference on Security Technology, Ottawa, Ont., 2007, pp. 80-84.

[9] Jan A. Jacobs, MD, PhD, Marc Van Ranst, MD, PhD, Biometric Fingerprinting for Visa Application: Device and Procedure Are Risk Factors for Infection Transmission, Journal of Travel Medicine, Volume 15, Issue 5, 1 September 2008, Pages 335–343.

[10] Hygiene not an issue for biometrics, Biometric Technology Today, Volume 15, Issues 11–12, 2007, pg. 3-4, ISSN 0969-4765.

[11] Biometric sensors no dirtier than doorknobs, Purdue University, October 10, 2007.

[12] Ghareeb PA, Bourlai T, Dutton W, McClellan WT. Reducing Pathogen Transmission in a Hospital Setting. Handshake verses Fist Bump: A Pilot Study. J Hosp Infect. 2013; 85:321–3. doi: 10.1016/j.jhin.2013.08.010



Further reading

Ethical Principles for Biometrics
https://www.biometricsinstitute.org/ethical-principles-for-biometrics/

NIST: Face Recognition Vendor Test Part 3: Demographic Effects (2019)
https://www.nist.gov/publications/face-recognition-vendor-test-part-3-demographic-effects

NIST: Guidance for Evaluating Contactless Fingerprint Acquisition Devices (2018)
https://www.nist.gov/publications/guidance-evaluating-contactless-fingerprint-acquisition-devices

NIST: Usability Testing of a Contactless Fingerprint Device: Part 1 (2016)
https://www.nist.gov/publications/usability-testing-contactless-fingerprint-device-part-1

NIST: New Test on the Effect of Masks on Face Recognition Accuracy
https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

Contact

This paper was compiled by the Academic Research and Innovation Group with input from other key stakeholders of the Biometrics Institute. If you have any questions or comments about this document, please email manager@biometricsinstitute.org

Disclaimer

The Biometrics Institute provides guiding material as a tool to help its members conduct due diligence. While the Institute has used reasonable care to ensure the accuracy of the material, due to the content and variable inputs during and after the process of implementing biometrics, the institute cannot be held accountable for outcomes or compliance. The material has been prepared for informational purposes only and is not intended to provide legal or compliance advice. Organisations should consult industry experts should they require advice on the technical, legal or compliance aspects of the material.